НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет електроніки
(повна назва інституту/факультету)

Кафедра акустичних та мультимедійних електронних систем
(повна назва кафедри)

«На правах рукопису»
УДК 621.397

«До захисту допущено»
Завідувач кафедри
(підпис) Сергій НАЙДА
(ініціали, прізвище)
“ 1” грудня 2020 р.

Магістерська дисертація

зі спеціальності (спеціалізації) 171 Електроніка (Електронні системи мультимедіа та засоби Інтернету-речей)
(код і назва спеціальності)

на тему: «Дослідження особливостей створення захищеної персональної інформаційної мережі житлового будинку ».

Виконала студентка II курсу, групи ДВ-92мп
(шифр групи)

Рой Юлія Володимирівна _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник к.т.н., доц. Трапезон К.О. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент доц. кафедри ЕПС доц., к.т.н. Михайлов С.Р. _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.

Студенка Рой Ю.В.

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут (факультет) Факультет електроніки
(повна назва)

Кафедра акустичних та мультимедійних електронних систем
(повна назва)

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою

Спеціальність (освітня програма) 171 Електроніка

(Електронні системи мультимедіа та засоби Інтернету речей)
(код і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри
(підпис) Сергій НАЙДА
(ініціали, прізвище)
«1» грудня 2020 р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Рой Юлії Володимирівні
(прізвище, ім'я, по батькові)

1. Тема дисертації «Дослідження особливостей створення захищеної персональної інформаційної мережі житлового будинку».

Науковий керівник дисертації к.т.н., доц. Трапезон Кирило Олександрович .
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

затверджені наказом по університету від «05 » листопада 2020 р. № 3241-с

2. Строк подання студентом дисертації 01.12.2020 р.

3. Об'єкт дослідження: персональна інформаційна мережа житлового будинку з програмними та програмно апаратними методами захисту .

4. Предмет дослідження (Вхідні дані – для магістерської дисертації за освітньо-професійною програмою): кількість квартир у житловому будинку -21; первинний захист користувачів мережі – firewall; тип сканеру вузлів мережі - Assuria Auditor

5. Перелік завдань, які потрібно розробити: визначити особливості з проектування захищеної персональної інформаційної мережі, зробити огляд мережевої безпеки(можливі вразливості , загрози та атаки), оцінити методи аналізу загроз та відповідно дослідити можливості рішення щодо усування потенційних загроз мережі.
6. Перелік графічного (ілюстративного) матеріалу: 15 слайдів презентації, основними назвами плакатів якої є сформульовані завдання, мета, постановка проблеми, особливості дослідження створення персональної інформаційної мережі житлового будинку на основі програмних та програмно – апаратних методів захисту.
7. Дата видачі завдання 1. 09. 2020 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
1	Розгляд ключових особливостей проектування захищеної персональної інформаційної мережі	1.09.2020 – 1.10.2020	Виконано
2	Аналіз мережевої безпеки, можливих загроз та атак; аналіз методів рішення та усунення вразливостей системи	2.10.2018 – 30.10.2020	Виконано
3	Вибір методів захисту для створення захищеної персональної інформаційної мережі житлового будинку	31.10.2020 – 1.12.2020	Виконано
4	Підготовка матеріалів до друку та оформлення пояснювальної записки	02.12.2020 – 05.12.2020	Виконано
5	Підготовка та оформлення презентації для доповіді	06.12.2020 – 12.12.2020	Виконано

Студентка _____ Юлія РОЙ
(підпис) (ініціали, прізвище)

Науковий керівник _____ Кирило ТРАПЕЗОН
(підпис) (ініціали, прізвище)

УДК 621.397

РЕФЕРАТ

Рой Ю.В. Дослідження особливостей створення захищеної персональної інформаційної мережі житлового будинку : магістерська дис. : 171 Електроніка. Київ, КПІ ім. Ігоря Сікорського, 2020. 92 с.

Магістерська дисертація: 92с, 25 рис, 2 дод., 22 табл., 35 джерел.

Ключові слова: захист мережі, проектування, програмні і апаратні методи захисту, тестування, мережа житлового будинку.

Актуальність дослідження. У сучасному світі активно розвиваються мережеві та інформаційні технології. Зараз неможливо в рамках міста знайти будівлю, де б не були розгорнуті підключення до мережі передачі даних на основі технологій Інтернету. Така мережа спрощує і оптимізує велику кількість задач, таких як обмін інформацією, робота над документами, користування програмами, обмін ресурсами та інформацією тощо. В якості такої будівлі доцільно розглянути житловий будинок на визначену кількість квартир. Інформація – це дуже цінний ресурс, тому зловмисники досить часто намагаються отримати доступ до мереж як корпоративних, так і домашніх. Основною причиною впровадження мережевої безпеки є захист мережі та системних ресурсів, підключених до мережі. Інформація в будь-якій формі вважається цінною властивістю мережі, і її втрата чи доступ до неї може коштувати грошей або в гіршому випадку, спричинить катастрофу. Зламування мережі може призвести до різних наслідків: перехоплення даних, зараження шкідливим ПЗ та знищенням усієї інформації.

Мета дослідження полягає в пошуку можливостей захисту персональної інформаційної мережі житлового будинку програмно-апаратним комплексом.

Завдання для досягнення мети: проаналізувати особливості проектування захищеної персональної інформаційної мережі, зробити огляд мережевої безпеки(можливі вразливості, загрози та атаки), оцінити методи аналізу загроз та відповідно дослідити можливості рішення щодо усування потенційних загроз мережі.

Об’єкт дослідження: захищена персональна інформаційна мережа житлового будинку.

Предмет дослідження: програмні та програмно апаратні методи захисту персональної інформаційної мережі.

Методи дослідження: алгоритми та методи, які визначені в основі функціонування систем та технологій в рамках захищеної локальної мережі, технології та алгоритми методів захисту локальних мереж.

Наукова новизна отриманих результатів: 1) запропоновані варіанти створення захищеної персональної інформаційної мережі; 2) запропоновано послідовний алгоритм налаштування програмних методів захисту персональної мережі.

Практичне значення одержаних результатів: результати роботи можуть бути використанні при проектуванні домашніх мереж та «будинкових» мереж багатоквартирних будинків.

SUMMARY

Master's dissertation: 92 p., 25 fig., 22 tabl., 2 supplements, 35 sources.

Keywords: network protection, design, software and hardware protection methods, testing, residential building network

Relevance of research. In the modern world, network and information technologies are actively developing. At present, it is impossible to find a building within the city where connections to the data network based on Internet technologies have not been deployed. This network simplifies and optimizes many tasks, such as information exchange, working on documents, using programs, exchanging resources and information, and more. As such a building, it is advisable to consider a residential building for a certain number of apartments. Information is a very valuable resource, so attackers often try to access both corporate and home networks. The main reason for implementing network security is to protect the network and system resources connected to the network. Information in any form is considered a valuable property of the network, and its loss or access to it can cost money or, in the worst case, cause a catastrophe. Hacking a network can lead to various consequences: data interception, malware infection and destruction of all information. Therefore, it is important to pay attention to network protection, search for vulnerabilities and identify potential threats that could harm the current system and resources.

The purpose of the study is to find opportunities to protect the personal information network of a residential building software and hardware.

Objectives to achieve the goal: to analyze the features of designing a secure personal information network, to review network security (possible vulnerabilities, threats and attacks), to evaluate methods of threat analysis and, accordingly, to explore the possibility of solving potential threats to the network.

Object of study: protected personal information network of a residential building.

Subject of study: software and hardware methods of personal information network protection.

Research methods algorithms and methods that are defined in the basis of the functioning of systems and technologies within a secure local area network, technologies and algorithms of local area network protection methods

Scientific novelty of the obtained results: 1) proposed options for creating a secure personal information network; 2) a sequential algorithm for configuring software methods for personal network protection is proposed

The practical implications of the findings: the results of the work can be used in the design of home networks and "home" networks of apartment buildings.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ASA 5505	-	Номер моделі 5505 Адаптивний пристрій захисту;
DNS	-	Domain Name System;
DoS attack	-	Denial of Service attack;
IoT	-	Internet of Things;
IPsec	-	Internet Protocol Security;
LAN	-	Local Area Network;
NAT	-	Network Address Translation;
PAT	-	Port Address Translation;
PDIOO	-	Plan Design Implement Operate Optimize;
PON	-	Passive Optical Network;
SSH	-	Secure Socket Shell;
SSID	-	Service Set Identifier;
VLAN	-	Virtual Local Area Network;
VPN	-	Virtual Private Network;
WEP	-	Wired Equivalent Privacy.

ВСТУП

У сучасному світі активно розвиваються мережеві та інформаційні технології. Зараз неможливо в рамках міста знайти будівлю, де б не були розгорнуті підключення до мережі передачі даних на основі технологій Інтернету. Така мережа спрощує і оптимізує велику кількість задач, таких як обмін інформацією, робота над документами, користування програмами, обмін ресурсами та інформацією тощо. В якості такої будівлі доцільно розглянути житловий будинок на визначену кількість квартир.

Ще з давніх часів люди охороняють свою власність. Відсутність охорони може спричинити втрату майна чи життя людини. З плином часу стала актуальною проблема захисту інформаційної та цифрової власності. Подібним чином комп'ютерні ресурси повинні бути захищені від внутрішніх і зовнішніх зловмисників.

Інформація – це дуже цінний ресурс, тому зловмисники досить часто намагаються отримати доступ до мереж як корпоративних, так і домашніх. Основною причиною впровадження мережевої безпеки є захист мережі та системних ресурсів, підключених до мережі. Інформація в будь-якій формі вважається цінною властивістю мережі, і її втрата чи доступ до неї може коштувати грошей або в гіршому випадку, спричинить катастрофу. Зламування мережі може призвести до різних наслідків: перехоплення даних, зараження шкідливим ПЗ та знищенням усієї інформації. Тому важливо приділити увагу захисту мережі, пошуку вразливостей та виявленню можливих загрози, які можуть завдати шкоди поточній системі та ресурсам. Тому сьогодні надзвичайно важливо, щоб компанії приділяли особливу увагу посиленню своїх рівнів безпеки.

Впровадження засобів контролю безпеки в мережевому середовищі дозволяє мережевій системі працювати належним чином. Основною причиною впровадження мережевої безпеки є захист мережі та системних ресурсів, підключених до мережі. Останнім часом інформаційні технології у тому числі і в межах приватного сектору зачіплюють таке поняття, як “розумний” будинок та технології Інтернету речей. Розглянемо базові особливості які привалюють у даному сегменті розвитку інформаційних технологій.

1 ОСОБЛИВОСТІ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ

З моменту появи терміна «Інтернет речей» мережі, що складаються з великої кількості пристроїв, які спілкуються між собою, стрімко розвиваються. Внаслідок цього, IoT [1] (Internet of Things) стає однією з основних технологій в сучасному суспільстві.

Міжнародний союз електрозв'язку (ITU), у своїх рекомендації «Огляд Інтернету речей» [1], описує Інтернет речей наступним чином:

«глобальна інфраструктура, що надає складні послуги завдяки з'єднанню фізичних і віртуальних речей на основі існуючих і нових функціонально сумісних інформаційно-комунікаційних технологій».

В основі поняття Інтернет речей лежить сукупність пристроїв, переважно безпроводових, які обмінюються інформацією безпосередньо або через посередників. Передані дані надходять в хмарне сховище, де зберігаються, обробляються, а після візуалізуються. Кінцевим споживачем інформації є людина [2].

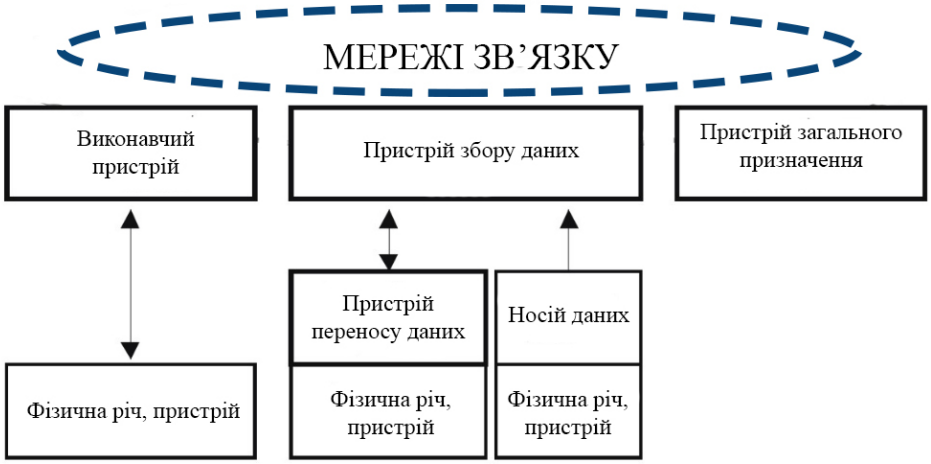


Рисунок 1.1 – Типи пристроїв Інтернету речей та їх взаємодія

Для побудови систем використовуються різні архітектури, радіо (проводові) технології, типи протоколів, які в сукупності визначають характеристики системи і її продуктивність. У свою чергу, технічні характеристики компонентів системи безпосередньо впливають на якість сервісу, вартість системи, її безпеку і керованість в цілому.

Застосування Internet of Things [1]. Не існує точних рамок або списку приладів, де можна застосувати систему Інтернету речей. На практиці IoT можна запровадити навіть в приватному будинку, оскільки практично будь-

який фізичний об'єкт можна перетворити в "розумний". Але якщо розібратися більш детально, то Інтернет речей можна впровадити:

- розумний будинок - з розумною системою кондиціонування або обігріву, розумним чайником або кавоваркою тощо;
- промисловість - програмні системи, сенсори, аналіз даних, розумні машини і обладнання;
- охорона здоров'я - медичні дрони, відкриття в генетиці, індивідуальний підхід до пацієнтів, аналіз роботи лікаря;
- агрокультура - прогноз кліматичних змін, обладнання для перевірки складу грунту, відстеження стану здоров'я тварин і навіть де знаходяться хворі тварини;
- ритейл - найпопулярніше це безконтактна оплата і спеціальні програми для покупок і доставки онлайн.

Крім перерахованих сфер, IoT також можна застосувати в енергетиці, для автомобілів, смартфонів і гаджетів, системи безпеки (в тому числі камери відеоспостереження) і звичайно ж - побудувати розумне місто [6].

1.1 Архітектура IoT

Повертаючись до рекомендацій ITU щодо Інтернету речей [1], можна знайти еталонну модель IoT: вона описує потрібні функції Інтернету речей та їх взаємодію між собою. Вона слугує основою для стандартизації [2].

Рисунок 1.2 – Еталонна модель IoT визначена ITU

IoT World Forum (IWF), тобто Всесвітній форум IoT, також працює над покращенням архітектури IoT. У 2014 році вони опублікували власну версію

основної моделі IoT [2], яка доповнює варіант ITU. Вона більш широко розглядає усі рівні архітектури, звертаючи увагу також на верхні рівні.

Рисунок 1.3 – Еталонна модель IoT визначена IWF [6]

Тобто, архітектура Інтернету речей – це сукупність пристроїв та контролерів (фізичний рівень пристроїв), що спілкуються за допомогою проводових і безпроводових сигналів (мережевий рівень), які передаються в хмарне сховище обробки даних.

1.2 Ключові протоколи персональної локальної мережі

Датчики та інші пристрої, підключені до Інтернету, потребують способів передачі і отримання інформації. В екосистемі Інтернету речей зв'язок з датчиком або виконавчим механізмом може здійснюватися по мідних проводах або безпроводовою персональною мережею регіону (WPAN). Це поширений метод промислового, комерційного та споживчого підключення до речей в Інтернеті.

Мережевий протокол - це встановлений набір правил, що визначають спосіб передачі даних між різними пристроями в одній мережі. По суті, це дозволяє підключеним пристроям обмінюватися даними незалежно від будь-яких відмінностей у їхніх внутрішніх процесах, структурі чи конструкції. Мережеві протоколи - це причина, через яку є можливість легко спілкуватися з людьми у всьому світі і, таким чином, відігравати важливу роль у сучасному цифровому зв'язку.

Мережеві протоколи дають можливість пристроям взаємодіяти один з одним через заздалегідь визначені правила, вбудовані в програмне та апаратне забезпечення пристроїв. Ні локальні мережі (LAN), ні глобальні

мережі (WAN) не можуть функціонувати так, як сьогодні, без використання мережевих протоколів.

Існує безліч різних каналів зв'язку між кінцевою точкою і Інтернетом. Одними з ключових стандартів безпроводового зв’язку в IoT є Bluetooth, Zigbee, Z-Wave і IEEE 802.15.4.

Основні протоколи, які використовуються в роботі мережі Інтернет наступні: TCP/IP, POP3, SMTP, FTP, HTTP, IMAP4, WAIS,WAP [8].

Мережеві протоколи працюють наступним чином: вони беруть широкомасштабні процеси і розбивають їх на невеликі, конкретні завдання або функції. Це відбувається на кожному рівні мережі, і кожна функція повинна взаємодіяти на кожному рівні, щоб виконати більш масштабне завдання. Термін набір протоколів відноситься до набору менших мережевих протоколів, що працюють спільно між собою.

Мережеві протоколи, як правило, створюються відповідно до галузевих стандартів різними мережевими або інформаційними організаціями.

Наступні групи визначили та опублікували різні мережеві протоколи:

- Інститут інженерів електрики та електроніки (IEEE)
- Робоча група з питань Інтернет-інженерії (IETF)
- Міжнародна організація зі стандартизації (ISO)
- Міжнародний союз телекомунікацій (MCE)
- Консорціум всесвітньої мережі (W3C)

Хоча моделі мережевих протоколів, як правило, працюють схожим чином, кожен протокол є унікальним і працює певним чином, детально описаним організацією, яка його створила.

Протоколи безпеки, які також називаються криптографічними протоколами, працюють над тим, щоб захистити мережу та передані через неї дані від несанкціонованих користувачів.

Загальні функції мережевих протоколів захисту включають наступне:

- Шифрування: протоколи шифрування захищають дані та захищають зони, вимагаючи від користувачів введення секретного ключа або пароля для доступу до цієї інформації.
- Аутентифікація: Протоколи автентифікації створюють систему, яка вимагає від різних пристроїв або користувачів мережі перевіряти свою ідентичність перед тим, як отримати доступ до захищених зон.
- Транспортування: Протоколи транспортної безпеки захищають дані під час їх транспортування з одного мережевого пристрою на інший [4].

1.2.1 IEEE 802.15.4

IEEE 802.15.4 - це стандартна бездротова персональна мережа, що відноситься до робочої групи IEEE 802.15. Модель є основою багатьох інших протоколів, включаючи Thread, Zigbee, Wireless HART і інші.

Архітектура IEEE 802.15.4. Протокол IEEE 802.15.4 працює в трьох діапазонах: 868 МГц, 915 МГц і 2400 МГц. Це зроблено для того, щоб мати широке географічне поширення: три різних діапазони і кілька методів модуляції. Смугою 2,4 ГГц користуються частіше всього,оскільки вища швидкість дозволяє використовувати коротші робочі цикли при передачі та прийомі, тим самим зберігаючи енергію. Також смуга 2,4 ГГц є популярною завдяки визнання на ринку технології Bluetooth.

Типовий діапазон протоколу 802.15.4 становить близько 200 метрів у відкритому режимі, з прямою видимістю. У приміщенні типовий діапазон становить близько 30 м.

Для розширення діапазону можна використовувати передавачі більшої потужності (15 дБм) або mesh-мережі. На рис. 1.3 показані три смуги, використовувані 802.15.4 та розподіл частот. 915 МГц використовується поділ частот 2 МГц, а в смузі 2,4 ГГц використовується поділ частот 5 МГц

Топологія IEEE 802.15.4. В IEEE 802.15.4 є два основних типи пристроїв. Перший тип, повнофункціональний пристрій (FFD) - підтримує будь-яку топологію мережі, може бути координатором мережі (PAN) і може зв'язуватися з будь-яким пристроєм PAN-координатором. Другий тип пристроїв: функціонально обмежений пристрій (RFD). RFD обмежений тільки топологією зірки, не може виконувати функції координатора мережі, може зв'язуватися тільки з мережевим координатором.

Зоряна топологія є найпростішою, але вимагає, щоб всі повідомлення між одноранговими вузлами проходили через координатор PAN для маршрутизації. Тимчасова топологія є типовою mesh-мережею і може безпосередньо зв'язуватися з сусідніми вузлами.

1.2.2 Zigbee

Zigbee - це протокол WPAN, заснований на IEEE 802.15.4, призначений для комерційних і житлових мереж IoT, що обмежені вартістю, потужністю і простором. Zigbee отримав свою назву від концепції бджолиного польоту.

Коли бджола летить туди-сюди між квітами, збираючи пилок, вона нагадує пакет, що проходить через mesh-мережу від пристрою до пристрою.

Zigbee заснований на 802.15.4, крім мережевих рівнів, подібних TCP / IP. Він може створювати мережі, виявляти пристрої, забезпечувати безпеку і управляти мережею. Він не надає послуги передачі даних або середу виконання додатків. Оскільки він по суті є mesh-мережею, то є самовідновлюваним та самодостатнім. Також Zigbee простий, вдалося вполовину скоротити підтримку програмного забезпечення за рахунок використання легкого стека протоколу.

У мережі Zigbee є три основних компоненти:

- контролер Zigbee (ZC) - високопродуктивний пристрій в мережі Zigbee, що використовується для формування і запуску мережевих функцій. Кожна мережа Zigbee буде мати один ZC, який виконує роль координатора PAN 802.15.4 2003 PF (FFD). Після формування мережі ZC може поводити себе як ZR (маршрутизатор Zigbee). Він може призначати логічні мережеві адреси і вирішувати вузлів приєднуватися чи залишати mesh-мережу;
- маршрутизатор Zigbee (ZR) - цей компонент є необов'язковим, але виконує деяке навантаження на мережеву стрибкоподібну перебудову і координацію маршрутизації. Він також може виконувати роль FFD і має зв'язок з ZC. ZR бере участь в маршрутизації повідомлень з декількома переходами і може призначати логічні мережеві адреси і вирішувати вузлів приєднуватися чи залишати mesh-мережу;
- кінцевий пристрій Zigbee (ZED) - зазвичай це простий термінал, наприклад, вимикач світла або термостат. Він має досить функціональних можливостей для спілкування з координатором. Проте не має логіки маршрутизації; тому будь-які повідомлення, що надходять на ZED, що не націлені на це кінцевий пристрій, просто передаються. Також не може виконувати асоціації.

Zigbee підтримує три основні топології (рис. 1.4):

- «зоряна» мережа - один ZC з одним або декількома ZED. Тільки розширює зв'язок між двома вузлами і тому обмежений на відстані вузла. Також потрібний надійний зв'язок з єдиною точкою відмови в ZC;
- кластерне дерево - мережа з декількома переходами, яка використовує маяк і розширює охоплення мережі і діапазон по мережі зірок. Вузли ZC і ZR можуть мати дочірні елементи, але ZED залишаються істинними кінцевими точками. Вузли-нащадки взаємодіють тільки зі своїм батьком.

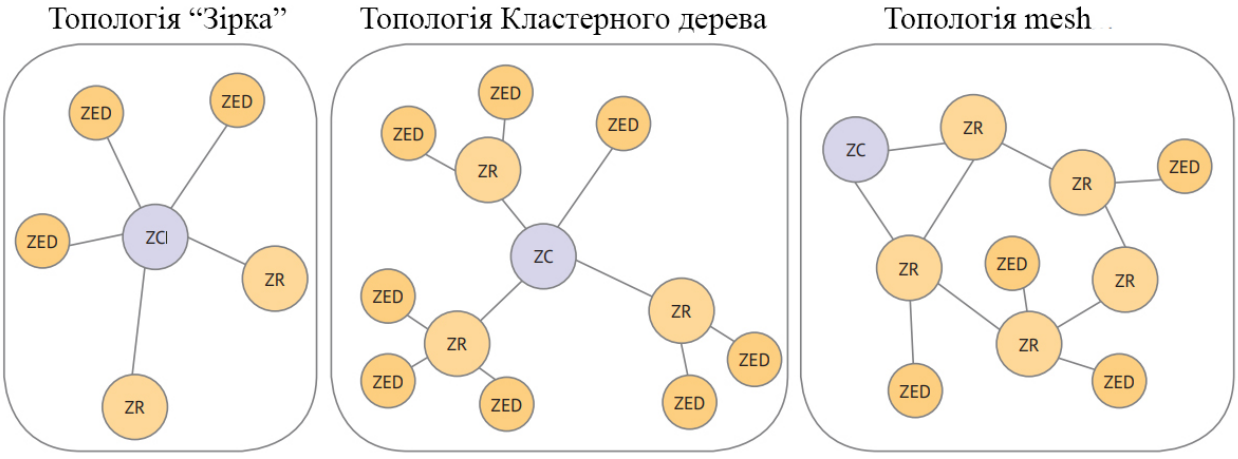
Батьки можуть спілкуватися вниз за течією зі своїми дітьми або вгору по потоку до свого батька. Все ще існує проблема в єдиній точці відмови в центрі;

- mesh-мережа - динамічне формування шляху і зміна форми. Маршрутизація може відбуватися з будь-якого початкового пристрою на будь-який цільовий пристрій. Використовує алгоритми маршрутизації дерева і таблиці. Радіостанції ZC і ZR повинні постійно бути запитана, щоб виконувати вимоги до маршрутизації, забираючи для цього час автономної роботи. Крім того, обчислення затримки в mesh-мережі може бути важким. Маршрутизатори в певному радіусі один від одного можуть безпосередньо зв'язуватися один з одним. Основною перевагою є те, що мережа може вирости за межі видимості і мати кілька додаткових шляхів.

Рисунок 1.4 – Три типи топології мережі Zigbee [2,6]

1.2.3 Z-Wave

Z-Wave [6] - це протокол WPAN, який використовується перш за все для споживчої і домашньої автоматизації. Близько 2100 продуктів використовують цю технологію. Він знайшов свій шлях в комерційних і



будівельних сегментах, в областях освітлення і управління HVAC. Що стосується частки ринку, Z-Wave не так популярний, як Bluetooth або Zigbee. Z-Wave - ще одна mesh-технологія в діапазоні 900 МГц. Z-Wave є закритим протоколом в більшості випадків з обмеженою кількістю виробників апаратних модулів.

Дизайн Z-Wave - це домашнє і споживче освітлення / автоматизація. Він призначений для використання з дуже низькою пропускною здатністю для зв'язку з датчиками і перемикачами. Проект заснований на стандарті

ITU-T G.9959 на рівні PHY і MAC. ITU-T G.9959 є специфікацією Міжнародного союзу електрозв'язку для короткодіючих вузькосмугових радіокомунікаційних приймачів в смузі частот нижче 1 ГГц.

В діапазоні частот до 1 ГГц є декілька піддіапазонів, які використовуються для Z-Wave в залежності від країни походження. У США центральна частота 908,40 МГц є стандартною. Існують три швидкості передачі даних, які Z-Wave може використовувати з різним розподілом частоти для кожного:

- 100 Кбіт / с - 916,0 МГц з діапазоном 400 кГц;
- 40 Кбіт / с - 916,0 МГц з діапазоном 300 КГц;
- 9,6 Кбіт / с - 908,4 МГц з діапазоном 300 КГц.

Кожна смуга працює на одному каналі.

Модуляція, яка виконується на рівні PHY, використовує частотну маніпуляцію для швидкості передачі даних 9,6 Кбіт/с і 40 Кбіт/с. При швидкості 100 Кбіт/с використовується гаусівська маніпуляція з частотним перемиканням. Вихідна потужність становитиме приблизно 1 мВт при 0 дБ.

З точки зору ролі і відповідальності мережа Z-Wave складається з різних вузлів з специфічними функціями [6]:

- контролер - це пристрій верхнього рівня забезпечує таблицю маршрутизації для mesh-мережі і є хостом / майстром mesh-мережі.

Існує два основних типи контролерів [3]:

- головний контролер - основний контролер є провідним, і тільки один майстер може існувати в мережі. Він має можливість підтримувати топологію і ієрархію мережі. Він також може включати або виключати вузли з топології. Він також зобов'язаний виділяти ідентифікатори вузлів;

- вторинний контролер - ці вузли допомагають головному контролеру з маршрутизацією;

- підпорядкований пристрій/вузол - ці пристрої виконують дії на основі команд, які вони отримують. Ці пристрої не можуть зв'язуватися з сусідніми підлеглими вузлами, за винятком випадків, коли це передбачено інструкцією з допомогою команди. Підпорядковані пристрої можуть зберігати інформацію про маршрутизацію, але не обчислювати або оновлювати таблиці маршрутизації. Як правило, вони будуть виступати в якості ретранслятора в mesh-мережі.

Топологія і маршрутизація Z-Wave. Топологія mesh-мережі Z-Wave показана на рис. 1.5, використовуючи деякі типи пристроїв і атрибути, пов'язані з підлеглими пристроями та контролерами. Один первинний контролер управляє мережею і встановлює поведінку маршрутизації.

Рівень маршрутизації в стеці Z-Wave управляє транспортуванням кадрів з одного вузла на інший. Рівень маршрутизації налаштовує правильний список ретрансляторів, якщо він необхідний, сканує мережу для змін в топології і підтримує таблицю маршрутизації. Таблиця досить проста і вказує, який сусід підключений до даного вузла. Вона відображає тільки один швидкий стрибок. Таблиця побудована головним контролером, задаючи кожному вузлу в mesh-мережі дані, які пристрої доступні з його місця розташування.

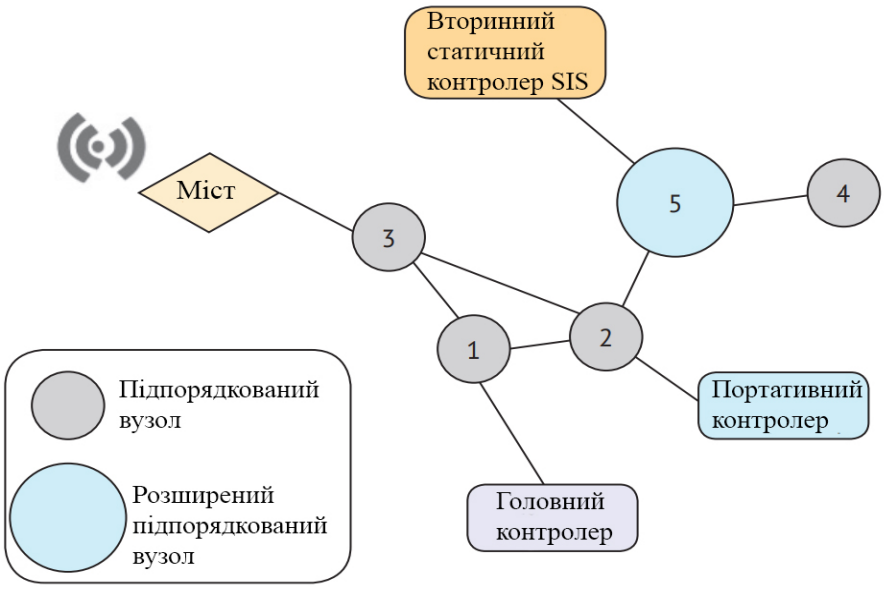


Рисунок 1.5 – Топологія мережі Z-Wave [6]

Z-Wave включає один основний контролер і чотири підлеглих пристрої і один розширений підпорядкований. Контролер моста виступає в якості шлюзу для мережі WiFi. Портативний контролер і додатковий контролер також розміщуються в mesh-мережі для допомоги основному контролеру.

1.2.4 SSH

Secure Socket Shell (SSH): Цей протокол забезпечує безпечний доступ до комп’ютера, навіть якщо він знаходиться в незахищеній мережі. SSH особливо корисний для мережевих адміністраторів, яким потрібно віддалено керувати різними системами.

SSH забезпечує автентифікацію на основі пароля або відкритого ключа та шифрує з'єднання між двома кінцевими точками мережі. Це безпечна альтернатива застарілим протоколам входу (наприклад, telnet, rlogin) та незахищеним методам передачі файлів (таким як FTP) [21].

Окрім надійного шифрування, SSH широко використовується адміністраторами мережі для віддаленого управління системами та додатками, доставки виправлень програмного забезпечення або виконання команд та переміщення файлів.

Протокол SSH вбудований у сервери Unix та Linux, щоб забезпечити безпечне з'єднання між системами. З'єднання встановлюється клієнтом SSH, який має намір підключитися до сервера SSH. Клієнт SSH ініціює процес налаштування підключення та використовує криптографію з відкритим ключем для перевірки ідентифікації сервера SSH. Після етапу налаштування протокол SSH використовує сильні симетричні алгоритми шифрування та хешування для забезпечення конфіденційності та цілісності даних, якими обмінюються клієнт та сервер.

Наведене нижче зображення, що представляє спрощений потік з'єднання SSH:

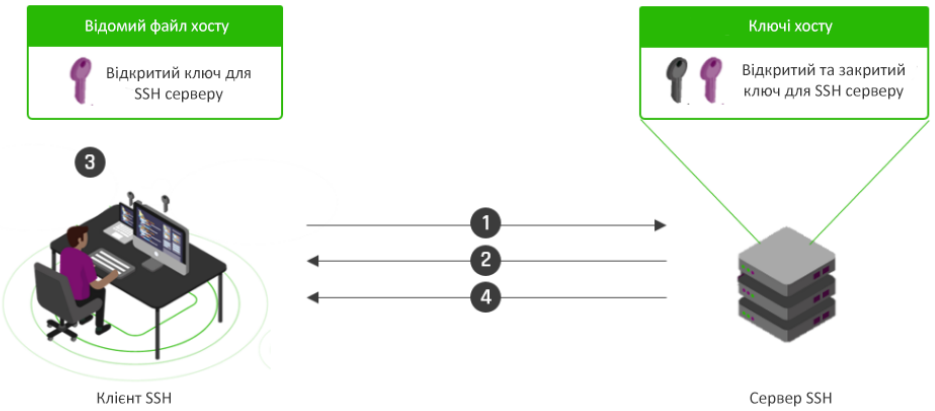


Рисунок 1.8 – Потік з’єднання SSH [2]

1. Клієнт ініціює підключення до сервера SSH.

2. Сервер надсилає клієнту свій відкритий ключ.

3. Відкритий ключ сервера зберігається у відомому файлі хостів клієнта.

4. Клієнт та сервер узгоджують параметри з'єднання та встановлюють з'єднання.

Під час налаштування з'єднання клієнт та сервер домовляються та узгоджують симетричний алгоритм шифрування, який буде використовуватися для їх зв'язку, та генерують ключ шифрування, який буде використовуватися.

Протокол SSH використовує стандартні сильні алгоритми шифрування, такі як AES, для забезпечення зв'язку між залученими сторонами. Крім того, протокол використовує алгоритми хешування, такі як SHA-2, для забезпечення цілісності переданих даних.

Протокол SSH дозволяє автентифікацію клієнта за допомогою традиційних паролів або автентифікації за відкритим ключем. Однак, враховуючи ризики та неефективність використання паролів, аутентифікація за відкритим ключем використовується ширше. Ключі SSH не тільки набагато сильніші за паролі, вони також дозволяють системним адміністраторам обійти потребу в ручному вході за паролем.

Як користувач автентифікується за допомогою ключів SSH? Вони генерують пару відкрито-приватних ключів із клієнтом SSH (наприклад, OpenSSH), використовуючи команду ssh-keygen. Після створення користувач розміщує свій авторизований ключ (відкритий ключ) у файлі санкціонованих ключів на сервері, до якого йому потрібно підключитися.

Коли користувач віддалено входить в систему за допомогою автентифікації на основі ключів, сервер OpenSSH шукає авторизовані ключі, а користувач автентифікується на сервері за допомогою відповідного приватного ключа.

Оскільки для цього не потрібна ручна автентифікація, автентифікація на основі ключів часто використовується для захисту випадків використання автоматизації IT-процесів, таких як безпечна автоматизована передача файлів, процеси резервного копіювання та копіювання або інструменти управління конфігурацією (тобто Ansible, Terraform, Chef або Puppet).

SSH-з'єднання в основному використовувались для захисту різних типів зв'язку між локальною машиною та віддаленим хостом, включаючи:

- Захищений віддалений доступ до ресурсів
- Віддалене виконання команд
- Доставка програмних виправлень та оновлень
- Інтерактивна та автоматизована передача файлів

На додаток до створення захищеного каналу між локальними та віддаленими комп'ютерами, протокол SSH використовується для управління критично важливою корпоративною інфраструктурою, такою як маршрутизатори, серверне обладнання, платформи віртуалізації та операційні системи.

Ключі SSH використовуються для автоматизації доступу до серверів і часто використовуються в сценаріях, системах резервного копіювання та

інструментах управління конфігурацією. Завдяки своїй конструкції, яка забезпечує можливість зв'язку через організаційні межі, ключі SSH забезпечують можливості єдиного входу (SSO), що дозволяє користувачам переходити між своїми обліковими записами, не вводячи пароль кожного разу.

Ключі SSH – це безпечне та ефективне управління. Проблема полягає в тому, що більшість організацій не знають про величезну кількість SSH-ключів, які вони мають, і тому ці ключі залишаються без відстеження та некерованими. Некеровані ключі піддають організації значним ризикам, які в гіршому випадку можуть вивести з ладу критичні інформаційні системи на місяці [22].

Клавіші SSH забезпечують той самий доступ, що і імена користувачів та паролі. Крім того, вони часто надають root-доступ до привілейованих облікових записів на рівні операційної системи, надаючи командний рядок. Вони також надають доступ до ресурсів - виробничих серверів, баз даних, маршрутизаторів, брандмауерів, систем аварійного відновлення, фінансових даних, платіжних систем, інтелектуальної власності та інформації про пацієнтів.

Отримавши зловмисний доступ, зловмисник означає, що він може робити що завгодно на сервері - включаючи введення шахрайських даних, підрив програмного забезпечення для шифрування, встановлення стійких шкідливих програм або відверте знищення системи. Конфіденційність, цілісність та безперервність операцій порушуються. Навіть якщо ключ дає некорневий доступ, уразливості ескалації локальних привілеїв часто можуть призвести до того, що зловмисник отримає root-доступ.

1.2.5 IEEE 802.1Q/ VLAN tagging

VLAN tagging - це метод, за допомогою якого на порту обробляється більше одного VLAN. VLAN tagging використовується, щоб визначити, який пакет належить до якої VLAN з іншого боку. Для полегшення розпізнавання пакет позначається тегом VLAN у кадрі Ethernet. Незалежні логічні системи можуть бути сформовані точно за допомогою позначення VLAN всередині самої фізичної мережі. За допомогою цієї системи тегів VLAN можна створити окремі домени.

Стандартний кадр IEEE 802.3 Ethernet має поле тип/довжини, а всі наступні стандарти зберегли однаковий формат кадру. Підхід, застосований

до стандарту VLAN (IEEE 802.1Q), полягав у запровадженні нового формату кадру [26].

Цей новий формат кадру показаний нижче з порівнянням із форматом кадру 802.3.

Новий формат кадру IEEE 803.1Q має два нових 2-байтових поля. Слідом за полями MAC-адреси джерела та призначення йде вихідне поле типу / довжини. Для цього поля встановлено значення 8100Hex, і оскільки це значення перевищує 1500, воно інтерпретується як значення типу, а 8100Hex вказує ідентифікатор протоколу VLAN.

Наступне 2-байтове поле складається з трьох підполів [8].

Перше - це поле 3-бітового пріоритету (PRI) і воно було введене для того, щоб дозволити (майбутнім) кадрам присвоїти значення пріоритету, щоб визначити послідовність, в якій передаються кадри.

Друге підполе називається ідентифікатором канонічного формату (CFI) і використовується для забезпечення можливості вбудовування кадру, що відноситься до локальної мережі Token, у поле даних цього кадру.

Третє підполе - це 12-розрядний ідентифікатор VLAN. Кожній робочій групі присвоюється різний ідентифікатор VLAN, і кожен кадр, переданий членами однієї робочої групи, має однаковий ідентифікатор у цьому полі.

Потім наступне 2-байтове поле - це нове поле довжини, і це вказує кількість байтів у полі даних.

Давайте розглянемо наступний малюнок, щоб ми могли чітко пояснити, як працює операція переадресації кадрів у VLAN [2].

Ця локальна мережа базується на мостових концентраторах, причому як найнижчий рівень із трьох концентраторів, так і єдиний концентратор у верхньому рівні, що відповідає стандарту IEEE 802.1Q. Крім того, усі комп’ютери в цій локальній мережі мають мережеві карти, які відповідають стандарту IEEE 802.1Q. Це означає, що всі вузли в цій локальній мережі генерують та обробляють кадри в новому форматі IEEE 802.1Q, як показано на попередньому малюнку.

Отже, кожному комп’ютеру присвоюється певний ідентифікатор VLAN, який вказує VLAN, до якого належить комп’ютер. Зверніть увагу, що цей ідентифікатор VLAN можна легко змінити, якщо стануть необхідними модифікації поточних робочих груп [8].

За стандартом кожен комп’ютер може бути ідентифікований або за номером порту, за MAC-адресою, а в деяких випадках за IP-адресою. IP-адреса знаходиться в полі даних кадру MAC, і, отже, може призвести до

проблем, якщо існують альтернативні формати мережевих адрес з IP. Крім того, оскільки номери портів, пов’язані з комп’ютером, змінюються при кожному переміщенні комп’ютера, це також може створювати проблеми. Отже, в більшості випадків кожен комп’ютер ідентифікується за своєю MAC-адресою.

Під час запуску міст дізнається номер порту, до якого приєднаний кожен комп'ютер, зчитуючи адресу джерела (MAC) у заголовку кожного кадру, отриманого в порту, перед тим, як кадр переадресовується на всі інші порти. Потім номер порту разом із відповідною MAC-адресою вводиться до таблиці маршрутизації мосту.

Цією ж процедурою дотримуються мостового концентратора, сумісного з IEEE 803.1Q, з додаванням того, що ідентифікатор VLAN у заголовку кожного кадру також вводиться в таблицю маршрутизації. Подібним чином, під час фази навчання, копія кадру передається до концентратора на вищому рівні, і це, в свою чергу, створює власну таблицю маршрутизації. Таблиці маршрутів чотирьох мостів також показані на малюнку вище.

Після завершення етапу навчання може розпочатися маршрутизація кадрів між кожною VLAN та всередині неї. Наприклад, якщо припустити, що ПК з MAC-адресою 52 надсилає кадр, скажімо, серверу з MAC-адресою 57, оскільки ідентифікатор VLAN однаковий як для ПК, так і для сервера, комутатор BH1 здійснює маршрутизацію безпосередньо без будь-якої подальшої передачі.

Якщо зараз ПК з MAC-адресою 58 та ідентифікатором VLAN зеленого надсилає кадр на сервер з MAC-адресою 67, BH1 спочатку перенаправляє кадр до BH0. Потім BH0 звертається до своєї таблиці маршрутизації і, визначивши, що сервер з MAC-адресою 67 також є членом VLAN Green, він пересилає кадр на порт 2.

Таким чином, кадри маршрутизуються не тільки на їх MAC-адресу, але й на їх ідентифікатор VLAN, і через це навантаження на загальну мережу значно зменшується за рахунок включення ідентифікатора VLAN. Крім того, якщо фрейм має ідентифікатор VLAN, який відрізняється від ідентифікатора в таблиці маршрутизації, фрейм відкидається, що покращує безпеку мережі. Ця сама процедура виконується як для широкомовних, так і для багатоадресних кадрів.

Кілька прикладів того, для чого можна використовувати VLAN [8]:

- Щоб відокремити трафік управління мережею від трафіку кінцевого користувача або сервера.
- Щоб ізолювати чутливу інфраструктуру, послуги та хости, такі як корпоративні користувачі, від запрошених.
- Для встановлення пріоритетів або впровадження правил якості обслуговування (QoS) для конкретних послуг, таких як телефони VoIP.
- Надавати мережеві послуги для різних клієнтів в Інтернет-провайдері, Центрі обробки даних або Офісній будівлі, використовуючи ту саму інфраструктуру комутатора та маршрутизатора.

Логічно відокремлювати групи хостів, незалежно від їх фізичного розташування - наприклад, дозволяючи співробітникам відділу кадрів спільно використовувати одну і ту ж підмережу мережі та отримувати доступ до одних і тих же мережевих ресурсів, незалежно від їх розташування в будівлі.

Визначення та використання терміна VLAN Tagging сильно варіюється залежно від того, який постачальник обладнання використовується. Для того, щоб обладнання, сумісне з 802.1Q, ідентифікувало, до якої VLAN належить пакет даних, до кадру Ethernet додається заголовок 802.1Q, який визначає ідентифікатор VLAN.

Цей тег ідентифікатора VLAN може бути доданий або видалений хостом, маршрутизатором або комутатором. Усередині мережі фізичні порти налаштовуються як без позначок або тегів для певної VLAN - визначаючи, приймати та пересилати трафік, що належить кожному ідентифікатору VLAN. Давайте детальніше розглянемо кожен з них.

Без тегів: VLAN, що не позначений тегами, також іноді називають "рідною VLAN". Будь-який трафік, який надсилається від хоста до порту комутатора, у якого не вказано ідентифікатор VLAN, буде призначений без тегів VLAN.

Цей параметр зазвичай використовується при підключенні хостів, таких як робочі станції або пристрої, такі як IP-камери, які не позначають власний трафік і потребують зв’язку лише на одній конкретній VLAN. Порт може одночасно налаштовувати лише одну безтегову VLAN.

Позначено: Присвоєння позначаного VLAN порту додає цей порт до VLAN, але весь вхідний та вихідний трафік повинен бути позначений ідентифікатором VLAN для переадресації. Хост, підключений до порту

комутатора, повинен мати можливість позначати власний трафік і бути налаштований на це з тим самим ідентифікатором VLAN.

Позначені VLAN (на відміну від Untagged) на порту, як правило, використовуються при підключенні до хосту, який потребує доступу до декількох мереж одночасно, використовуючи один і той же інтерфейс, наприклад, сервер, що надає послуги більш ніж одному відділу в офісі. Він також може бути використаний при підключенні двох комутаторів, щоб обмежити доступ до VLAN для хостів, підключених до комутатора низхідної лінії зв'язку для цілей безпеки.

Магістраль: Магістральний порт зазвичай вважається членом усіх VLAN-мереж - він приймає та пересилає трафік на будь-який ідентифікатор VLAN і зазвичай налаштовується для портів висхідної та низхідної ліній між комутаторами та маршрутизаторами.

Незважаючи на те, що кожна родина продуктів Ubiquiti використовує різний підхід до налаштування VLAN, вони всі дотримуються одного і того ж методу без позначок, позначок, магістралей для управління трафіком і є сумісними.

1.3 Система «Розумний дім»

Розумні будинки стали дуже активною темою досліджень в останні десятиліття. Вчені та приватні корпорації у всьому світі працюють над цією системою: в першу чергу для полегшення життя мешканців, або для надання послуг певній цільовій аудиторії. Багато хто вважає, що розумні будинки можуть експлуатуватися для надання послуг підтримки особам з певними хворобами або порушеннями [7].

Розумний будинок - це будинок з автоматизованими системами, такими як функції управління освітленням та опаленням. Слово «розумний» широко використовується для будь-яких технологічних особливостей будинку, які можуть автоматизувати прості завдання. В даний час до системи можуть бути включені майже будь-які електричні компоненти будинку: зараз доступний широкий спектр датчиків для громадських будівель та житлових будинків.

Розумні будинки використовуються для кількох цілей. Вони можуть покращити комфорт вдома, зменшити споживання енергії та забезпечити автоматизацію домашніх справ. Вони можуть забезпечити найрізноманітніші алгоритми дій пристосувавши свою поведінку до вподобань мешканців.

Однак багато вчених вірять, що сфера розумних будинків повністю розкриє свій потенціал надаючи моніторинг стану людини та медичну допомогу.

Система "Розумний будинок" - це програмно-апаратний комплекс для автоматичного управління домашніми системами і пристроями. В системі використовується інтегрований в абонентські пристрою контролер Z-wave, який дозволяє створити мережу бездротових датчиків, керовану користувачем зі смартфона, планшета або веб-браузер [7].

Пристрої управління. Система "Розумний будинок" дозволяє об'єднувати всі комунікації і здійснювати управління датчиками з одного пристрою. Універсальним пультом управління розумного будинку може стати будь-який мобільний пристрій на основі iOS або Android з установленим на ньому додатком "Розумний будинок". Додаток доступний для безкоштовного скачування в App Store і Google Play.

Можливості системи "Розумний будинок"

- Забезпечення безпеки в приміщенні (система віддаленого спостереження, система виявлення задимлення, тощо);
- Для максимального комфорту і зручності все обладнання можна запрограмувати на послідовну або одночасну роботу в потрібному режимі із зазначенням часу і дати (керування мікрокліматом, освітленням, роботою електроприборів, тощо);
- Для раціонального користування послугами побутового постачання в системі є датчики обліку споживання ресурсів.

Для дистанційного контролю і управління стану датчиків системи, існує розсилка повідомлень на встановлений додаток мобільного пристрою [7].

Отже, система «розумний» будинок є технологічним застосуванням Інтернету речей. Використовуючи безпроводовий протокол Z-Wave, усі датчики успішно спілкуються один між одним, виконують потрібні алгоритми і сценарії. На рис.1.8 зображений приклад застосування та організації комунікаційного обладнання.

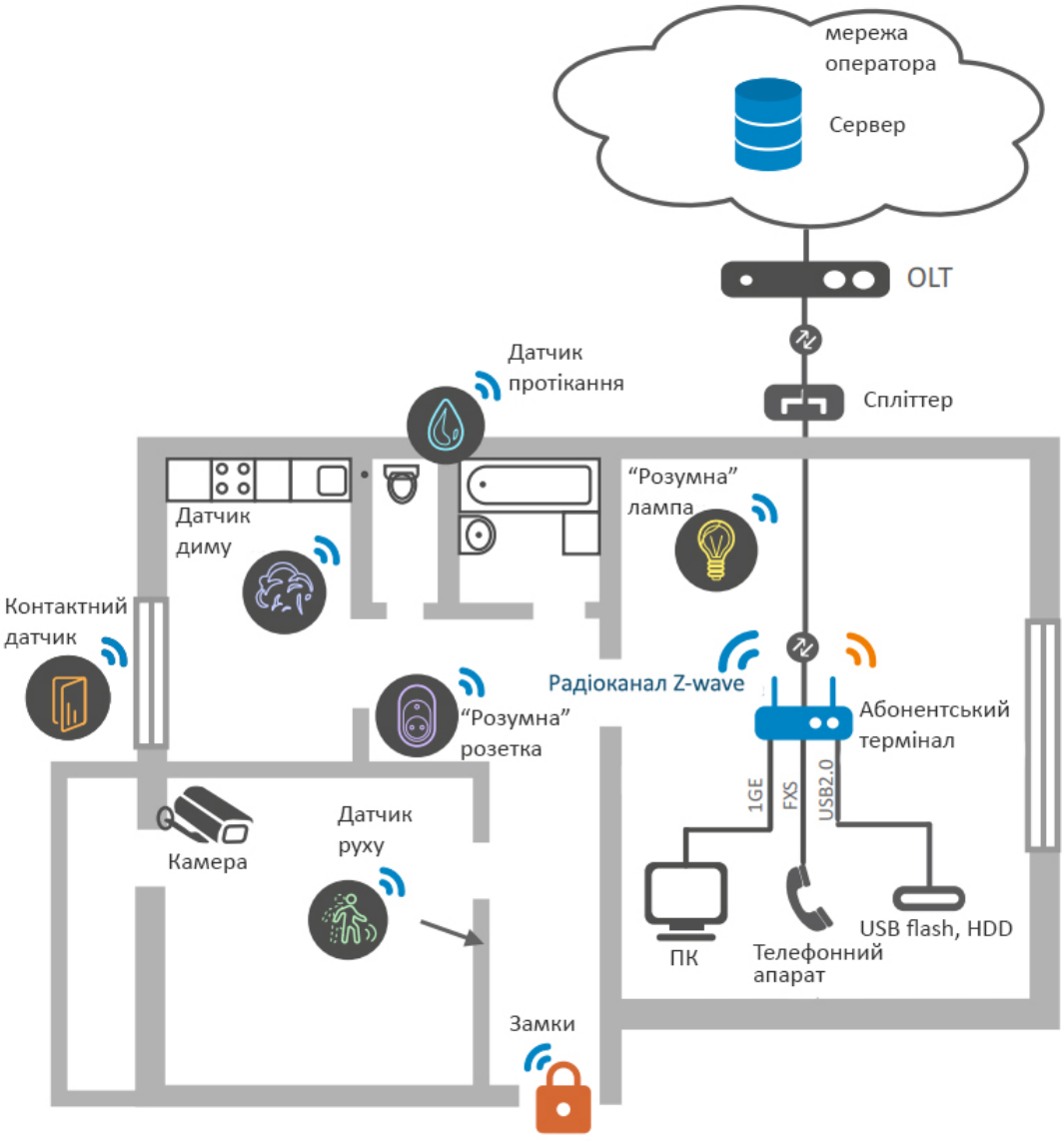


Рисунок 1.9 – Схема організації системи «розумний» дім

Висновки до розділу 1.

В цьому розділі розглянуто архітектуру Інтернету речей та перший крок в доставці даних пристроями IoT. Першим кроком в підключенні мільярдів пристроїв є використання правильних засобів зв'язку для доступу до датчиків, об'єктам і виконавчих пристроїв, щоб отримати виконання дій. Це роль бездротової персональної мережі. Описані мережі, такі як базовий протокол IEEE 802.15.4, Zigbee і Z-Wave. Вони найчастіше використовуються в системі "розумний " дім. Система "розумний" дім - це одне з втілень IoT. Дана система це це програмно-апаратний комплекс для автоматичного управління домашніми системами і пристроями.

2 БЕЗПЕКА ІНТЕРНЕТУ РЕЧЕЙ

2.1 Проблеми безпеки Інтернету речей

Інтернет речей (IoT) - нова технологія, яка вважається майбутнім Інтернету. Вона дозволяє пристроям/речам самостійно конфігурувати можливості на основі стандартних та сумісних протоколів зв'язку до ідентифікаційних даних та використовувати інтелектуальні інтерфейси через динамічну глобальну мережеву інфраструктуру. Концепцію IoT можна розглядати як продовження існуючої взаємодії між людьми та пристроями, що спілкуються через новий вимір. Завдяки вдосконаленням мереж зв'язку: мобільний зв’язок, інновації ідентифікації радіочастотних частот (RFID) та бездротові сенсорні мережам (WSN), речі та механізми в Інтернеті речей можуть взаємодіяти між собою незалежно від часу, місця чи форми [1].

Основним проривом IoT є формування інтелектуального середовища: розумні будинки, розумний транспорт, розумні товари, розумні міста, розумне здоров’я тощо. Крім того, в перспективі бізнесу IoT має величезний потенціал для різних типів організацій та компаній, включаючи програми та постачальники послуг IoT, постачальників та інтеграторів платформ IoT, операторів зв'язку та постачальників програмного забезпечення. Більше того, IoT матиме надзвичайний вплив на процес навчання; особливо у системі вищої освіти.

Зі стрімким збільшенням використання додатків IoT різко порушилось декілька питань безпеки. Оскільки пристрої та речі стають частиною Інтернет-інфраструктури, то потрібно бути впевненими у їх захищеності. Коли майже все буде під’єднано до Інтернету, ця проблема стане більш помітною; при постійному глобальному впливі в Інтернеті буквально виявиться більше незахищених аспектів. Це неконтрольоване середовище буде згодом використане хакерами, тобто це вплине на масове зловживання пристроями IoT. Крім того, IoT також збільшить потенційні поверхні для атаки хакерів та інших кіберзлочинців [4].

Дослідження, проведене Hewlett Packard [3], показало, що 70% найбільш часто використовуваних пристроїв IoT містять серйозні вразливості. Пристрої IoT є вразливими до загроз безпеки через свою конструкцію та шляхи функціонування, через відсутність певних функцій безпеки, таких як незахищений носій зв'язку, недостатня конфігурація автентифікації та авторизації.

Іот має важчі проблеми забезпечення безпеки, в порівнянні з попередніми мережами. Це пов’язано з тим, що з’єднані різні топології мереж до яких під’єднано велику кількість об’єктів. Це призводить до низки нових потенційних ризиків щодо інформаційної безпеки та захисту даних, які слід враховувати. В першу чергу, на мережевому рівні найважчі проблеми безпеки: масштабованість мережі (непередбачений об’єм передачі даних від великої кількості вузлів). Окремо можна зазначити проблеми на програмному рівні: неминучі помилки в комплексному багаторівневому програмному забезпеченні, помилки у ядрі програми, застосування незахищеного коду. Крім того, відсутність безпеки створить опір прийняттю IoT компаніями та приватними особами.

Проблеми та складності безпеки можна вирішити, забезпечивши належну підготовку розробників щодо інтеграції рішень безпеки у продукти Інтернету речей і, таким чином, заохочуючи користувачів використовувати функції безпеки IoT, які вбудовані в пристрої [6].

2.1.1 Аспекти безпеки

Термін безпека охоплює широкий спектр різних понять. По-перше, це стосується базового забезпечення служб безпеки, включаючи конфіденційність, аутентифікацію, цілісність, авторизацію, невідмовність та доступність. Ці служби безпеки можуть бути реалізовані за допомогою різних криптографічних механізмів, таких як блокові шифри, хеш-функції або алгоритми підпису. Для кожного з цих механізмів надійною інфраструктурою управління ключами є фундаментальне значення для обробки необхідних криптографічних ключів [8].

Однак у контексті IoT безпека повинна зосереджуватись не лише на необхідних службах безпеки, але й на тому, як вони реалізуються в загальній системі, і як виконуються функції захисту. Для цього використовується наступна термінологія для аналізу та класифікації аспектів безпеки в IoT [6]:

- Архітектура безпеки відноситься до елементів системи, що бере участь в управлінні відносинами захисту між пристроями, і способи обробки цих взаємодій безпеки (наприклад, централізована або розподілена) під час життєвого циклу пристрою.
- Модель захисту вузла описує, як параметри безпеки, процеси та програми керуються в пристрої. Сюди входять аспекти, такі як процес поділу, безпечне зберігання ключових матеріалів тощо.

- Початкове завантаження системи безпеки означає процес, за допомогою якого пристрій надійно приєднується до IoT у певному місці та в певний момент часу. Завантажувальна передача включає аутентифікацію та авторизацію пристрою, а також передачу параметрів захисту, що дозволяють надійно працювати.
- Мережева безпека описує механізми, що застосовуються в мережі для забезпечення надійної роботи IoT. Зокрема, це запобігає зловмисникам змінювати або загрожувати роботі мережевих пристроїв. Безпека мережі може включати ряд механізмів, починаючи від безпечної маршрутизації і закінчуючи рівнем передачі даних та захистом мережевого рівня.
- Безпека додатків гарантує, що лише довірені екземпляри програми, що працює в Інтернеті речей, можуть взаємодіяти між собою, тоді як нелегітимні екземпляри не зможуть втручатися.

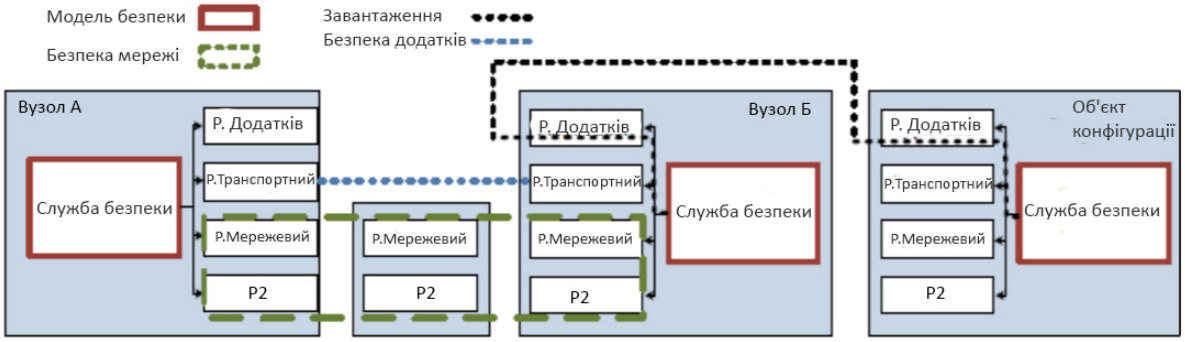


Рисунок 2.1 - Огляд механізму безпеки

2.2 Основні способи несанкціонованого доступу

Під основними способами несанкціонованого доступу до комп'ютерної інформації зазвичай розуміють такі [5]:

- несанкціонований доступ до інформації на фізичному носії
- методи подолання парольного захисту;
- перехоплення інформації в каналах зв'язку;
- використання недоліків програмного коду для отримання доступу до інформації
- впровадження шкідливого програмного коду
- нав'язування небезпечною передачі інформації;
- використання апаратних закладок;

- перехоплення побічних електромагнітних випромінювань і наведень (ПЕМВН), та інші.

Такий поділ є умовним, оскільки практично кожен з наведених способів може в певних випадках виступати складовою частиною будь-якого іншого з перерахованих.

Апаратні закладки — це спеціальні мікросхеми, які виконують ті ж функції по зніманню даних в комп'ютерній системі.

Крім того, перехоплення аудіо- та відеоінформації може здійснюватися за допомогою технічних засобів, розміщених в тому ж приміщенні, що і комп'ютер.

Проблемі перехоплення побічних електромагнітних випромінювань і наведень (ПЕМВН) в сучасній літературі приділяється велика увага з огляду на важливість цього технічного каналу витоку інформації. Варто відзначити, що найсильніші електромагнітні випромінювання утворюються від сигналів з виходу карти системного блоку, для яких випадковою антеною служить кабель, що йде до монітора. Для перехоплення цієї інформації достатньо мати приймальний пристрій, що працює в діапазоні частот 50500 МГц, спеціальний блок узгодження і портативний комп'ютер типу Notebook. Дальність перехоплення інформації таким комплексом складає 100-150 м.

2.3 Перехоплення інформації в каналах зв'язку

Для взаємодії між мережевими вузлами в комп'ютерних мережах використовуються різні середовища передачі. Будь-яка з них представляє інтерес з боку зловмисника для несанкціонованого знімання інформації.

Провідні мережі передачі даних мають очевидні особливості, що дозволяють порушнику безпеки виробляти знімання інформації за допомогою точних приладів, які вловлюють побічні електромагнітні випромінювання, які супроводжують будь-яку передачу по проводових мережах на основі мідного кабелю. Також зловмисник може призвести розпаралелювання проводового носія мережі зв'язку і безперешкодно виробляти отримання потоків даних, що циркулюють. У зв'язку з великою довжиною дротових мереж забезпечити належний фізичний контроль за каналом зв'язку не завжди є можливим. Тому розраховувати на будь-який захист від фізичного прослуховування недоцільно [5].

Безпроводова мережа передачі даних в силу своєї специфікації поширюється без використання проводових елементів і може бути легко

зареєстрована зловмисником на відстані, особливо з огляду на той факт, що найчастіше зона прийому безпроводової мережі поширюється за межі периметра безпеки організації. Тому пред'являються підвищені вимоги до безпроводової передачі, оскільки для доступу до середовища не потрібен ні фізичний доступ, ні спеціальні засоби для знімання побічного випромінювання.

До недавнього часу канали передачі даних, засновані на використанні оптичного сигналу як носія інформації, вважалися безпечними, оскільки вважалося вкрай скрутним знімання інформації без порушення цілісності каналу. В даний час є ряд науково-практичних робіт з даної тематики, що описують можливість з використанням відповідних технічних методів отримання інформації, що циркулює по оптичному кабелю.

Використання недоліків програмного коду для отримання доступу до інформації. Складність програмних продуктів, що забезпечують роботу комп'ютерних систем, стає більшою. У цих умовах розробники не завжди в змозі забезпечити достатній рівень тестування для виправлення всіх помилок програмного забезпечення. У числі інших помилок зустрічаються проблеми додатків з безпекою функціонування, які ведуть до появи вразливості. Порушники безпеки можуть скориставшись вразливістю отримати несанкціонований доступ до даних. Залежно від уразливості способи отримання доступу до інформації різні. Це може бути просто недостатня перевірка автентичності користувача при запиті певних даних, невірна перевірка справжності і т.д [8].

Частина проблем з безпекою функціонування мережевих додатків може бути пов'язана з невірним налаштуванням. Це викликано перш за все тим, що складність додатків з кожним днем тільки зростає. Вибір невірних параметрів настройки фахівцями частково ліквідується постачальниками програмного забезпечення шляхом установки початкових налаштувань в найбільш безпечний стан, але це не повністю вирішує проблеми зниження безпеки при подальшому виборі невірної конфігурації.

Іншим аспектом, пов'язаним з супроводом роботи комп'ютерних систем, є використання програмного коду не за призначенням. Це неправильний вибір технічним персоналом інструментів для виконання поставлених перед ним завдань. Для мінімізації ризиків невірного вибору програмних продуктів корисно залучати до вирішення завдань якомога більше фахівців широкого профілю. Також буває корисно користуватися

послугами аудиторських організації, здатних видати експертний висновок по використовуваному програмному рішенню.

Впровадження шкідливого програмного коду. Для отримання несанкціонованого доступу до інформації зловмисники можуть залучити шкідливий програмний код. Основний метод містить виконання програмного коду на системі, що атакується, спроектованого хакерами таким чином, щоб забезпечити доступ до інформації на комп'ютерній системі. Відповідно до способу впливу шкідливого коду на цільову систему можна виділити кілька варіантів поширення [8]:

- використання вразливостей в мережевих службах комп'ютерної системи;
- за допомогою спеціальних повідомлень електронної пошти;
- виконання скриптів на веб-сайтах при їх відкритті веб-браузером;
- використання флеш-накопичувачів з недостовірних джерел з використанням функції автозапуску;
- інші способи впровадження шкідливого коду.

У службах, які забезпечують взаємодію з мережі з іншими комп'ютерними системами, часто виявляються вразливості, які можуть бути використані зловмисниками для проникнення в цільову систему і надалі дозволяти їм виконувати зловмисний код.

При цьому шкідливий код може набувати різних видів. Детальна класифікація проводиться антивірусними компаніями, мета яких написання програмних продуктів, що займаються активною протидією такого роду атак на комп'ютерні системи.

Широке поширення комунікацій користувачів корпоративних мереж за допомогою пересилання електронних повідомлень зумовили привабливість поширення шкідливого коду за допомогою електронної пошти. Психологічний прийом, який базується на використанні поля «Від кого», де міститься ім'я відомого користувачеві людини, призводить до повної довіри до відправника з боку користувача. Він, не замислюючись про наслідки, відкриває лист і вкладення і тим самим несвідомо виконує шкідливий код. Недолік електронної пошти у вигляді можливості підробки адреси відправника широко використовується зловмисниками. За умови використання застарілої версії поштового клієнта іноді досить лише відкрити лист, щоб спровокувати виконання скрипта, вбудованого в код письма, що експлуатує уразливість поштового клієнта.

Використання веб-ресурсів для отримання інформації відкрило широкі можливості поширення шкідливого коду зловмисниками. Для цього

порушнику безпеки необхідно залучити користувача на інфіковану сторінку, а далі на ній виконається на стороні комп'ютера-жертви скрипт, який реалізує можливість для зловмисника маніпулювати даними користувача. Якщо раніше текст сторінки були тільки її уявленням на екрані, то тепер це складний механізм взаємодії програмного коду і візуального представлення, причому програмний код може виконуватися як на стороні веб-сервера, так і на стороні клієнта — веб-браузера. Цим і користуються зловмисники, винаходячи все нові способи запуску шкідливого коду на комп'ютерній системі користувача.

Застосування флеш-накопичувачів все ще залишається одним із способів передачі інформації між користувачами в комп'ютерних мережах. Вбудований механізм поширених операційних систем для автоматичного програвання вмісту і автозапуску зумовленого файлу на змінних носіях викликає запуск шкідливого коду відразу після підключення флеш-накопичувача до комп'ютерної системи. При цьому ніякої інтерактивності з користувачем не дотримується - все відбувається в автоматичному режимі. Таким чином, шкідливих код поширюється між комп'ютерними системами простим підключення знімних носіїв.

До інших менш використовуваним видам поширення шкідливого коду можна віднести застосування драйверів пристроїв для вбудовування коду зловмисника. Після установки драйвера в операційній системі відбувається запуск шкідливої програми.

Також можна відзначити окремо цілий клас програм, що маскуються під корисні програми. У реальності вони є тільки оболонкою, забезпеченою компонентами, які виконують шкідливі функції. Широке поширення отримали в даному напрямку псевдо антивірусні програми, установка яких не несе ніякої практичної користі, а за описом ховається програмний код зловмисника.

Примушення до використання небезпечних каналів передачі інформації. Дії зловмисника щодо отримання доступу до інформації, що обробляється засобами обчислювальної техніки, можуть полягати в застосування методик, спрямованих на примушування передачі інформації небезпечним способом [24]. Суть методу полягає в зміні схеми взаємодії мережевих додатків таким чином, щоб вся передача даних проводилася через мережевий вузол зловмисника. При цьому всю інформацію він в змозі прочитати і при бажанні змінити. Для реалізації такої атаки можна скористатися наступними недоліками роботи в комп'ютерних мережах:

- недоліки мережевих протоколів;
- помилки в архітектурі мережевих додатків;
- недоліки алгоритму шифрування переданих даних.

Багато з існуючих протоколів мережевої взаємодії не мають функції щодо захисту даних, що передаються від порушення їх конфіденційності, цілісності та доступності. Для проведення атак зловмисник вивчає принципи функціонування протоколу, за допомогою якого проводиться передача інформації, що цікавить. Потім, скориставшись недоліками реалізації протоколу, виробляє дії зловмисного характеру. Можна виділити кілька способів використання недоліків. Перший являє собою використання зловмисниками помилок в роботі мережевих протоколів. Шляхом взаємодії з мережевою службою можна викликати перехід мережевого протоколу на роботу за резервною схемою, яка, наприклад, не забезпечує шифрування даних, або не виробляє перевірку довіри до транзитних вузлів і т.д. Іншими словами, виконує вплив на мережеву службу, яка веде до використання менш безпечного способу передачі даних. Також сюди можна віднести помилки реалізації обробки невірно сформованих пакетів даних стеком протоколів операційної системи. У цьому випадку можливо порушення доступності роботи служби шляхом виведення її з ладу [8].

Другий спосіб полягає в наявності помилок в архітектурі додатків. До них відноситься можливість зміни будь-яких зовнішніх факторів, які знаходяться під управлінням зловмисника з метою переходу роботи протоколу в небезпечний режим. Під зовнішніми чинниками мається на увазі формування побічного впливу шляхом пересилання спеціально сформованих пакетів. Прикладом може служити робота протоколів маршрутизації, які на основі вивчення відповідей від сусідніх маршрутизаторів формують записи про можливі шляхи проходження трафіку. Зловмисник, підміняючи відповіді від маршрутизаторів, може створити таку конфігурацію мережі в пам'яті маршрутизатора, коли весь потік даних буде передаватися через спеціальних вузол порушника.

Іншим прикладом є посилка спеціальних пакетів при роботі протоколів, які змушують або користуватися сервісами посередників, якими будуть вузли зловмисника, або просто проводити дії, що призводять до порушення нормальної роботи мережевих служб. Наприклад, посилка повідомлень про закриття сеансу зв'язку в протоколі TCP (пакет зі встановленим прапором FIN), якщо такий пакет буде оброблений вузлом-жертвою, то сеанс буде закрито, і передачу доведеться починати спочатку.

Ще один приклад пов'язаний з роботою мережевих пристроїв локальної мережі, а саме обробка таблиць MAC адрес в комутаторах локальної мережі. Зловмисник за допомогою пересилання більшого числа пакетів з різними MAC адресами переповнить таблицю відповідності мережевих інтерфейсів і MAC адрес (MAC таблицю), що викличе пересилання всіх пакетів на всі порти. За умови фізичного підключення зловмисника до комутатора він зможе отримати всі мережеві пакети, циркулюючі через виведений з ладу комутатор [5].

Помилки в реалізації алгоритмів шифрування даних, що передаються, призводять до того, що вся інформація, що передається, стає доступна зловмисникові. Час від часу з'являється інформація про те, що той чи інший мережевий протокол, який використовує шифрування більше не є безпечним. Зазвичай це результат дослідження фахівців з інформаційної безпеки на предмет коректності його використання в потенційно небезпечних середовищах передачі. Крім того можлива поява вразливості в мережевому протоколі при використанні його в середовищі передачі, для якої він спочатку не проектувався.

Не так давно було продемонстровано отримання даних з шифрованого трафіку бездротової мережі, який використовує протокол WPA. Не виключено, що протоколи які зараз є стійкими до злому, незабаром будуть переведені в розряд некриптостойкіх.

2.4 Криптографічні методи і засоби захисту

Кіберзлочинність зростає з кожним днем, враховуючи цю проблему посилення методів мережевої безпеки також стає дуже важливим. Криптографія - один із найкращих способів забезпечити безпеку в мережі. Концепції алгоритму криптографії засновані на математиці. Криптографічні методи поділяються на дві основні категорії: симетричні та асиметричні [26].

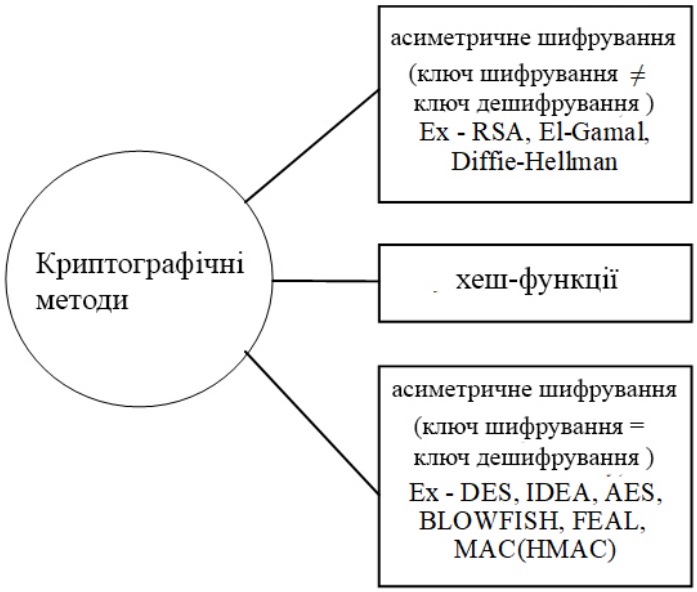


Рисунок 2.1 – Криптографічні методи

Криптографія не така проста у розробці. Досить складно писати методи шифрування та дешифрування при зміні одного біта. Криптограф використовує секретні коди для перетворення відкритого тексту в текст шифру, а також навпаки. Перший процес перетворення відкритого тексту в текст шифру називається технікою шифрування, а перетворення тексту шифру в звичайний текст - технікою дешифрування. Секретний код, який використовується криптографом для перетворення відкритого тексту, називається ключовим. Ключем може бути приватний ключ або відкритий ключ.

Наприклад, оскільки особа "A" має відкритий ключ, який доступний публічно для доступу. Припустимо, кожен, хто хоче надіслати дані особі "A", буде використовувати цей відкритий ключ для шифрування даних та надсилання до "A". Цей текст шифру можна розшифрувати лише за допомогою закритого ключа "A". Коли особа "B" використовує ключ для шифрування тексту і ділиться цим ключем з особою "A", використовуючи цей ключ, особа "A" може розшифрувати текст шифру. Це концепція приватного ключа, яка є конфіденційною та передається між лише відправнику та одержувачу. Коли один і той же ключ використовується для шифрування та дешифрування тексту, він називається симетричною криптографією, а коли різні ключі використовуються для шифрування та дешифрування коду, це називається асиметричною технікою криптографії [5].

Захист може бути реалізований як на програмному, так і на апаратному рівні. В середовищі IoT довіряти будь-якому об’єкту є складним завданням. Більшість питань безпеки IoT однакові як і для Інтернет-мережі, але вплив може бути різним. Але деякі проблеми можуть викликати серйозні проблеми в IoT, але їх не існує в Інтернет-мережі. Впровадження рішень безпеки в програмному забезпеченні набагато простіше і ремонтопридатніше порівняно з апаратними рішеннями. Впровадження криптографічних методів можливе як на апаратному, так і на програмному рівні. Криптографічні методи в основному легше застосувати на програмному забезпеченні, але програмну реалізацію легше загартувати, оскільки вони працюють на верхньому рівні операційної системи.

Замість традиційних методів криптографії в середовищі IoT для розумних об'єктів використовується криптографія LightWeight (LWCRYPT). Існують різні методи LWCRYPT, які ми можемо використовувати для безпеки IoT.

LWCRYPT [21] використовує концепцію мінімального використання доступних та важливих ресурсів для завершення роботи цільового джерела. Термін LightWeight (легкий) стосується використання алгоритму мінімального розміру з низьким споживанням енергії та потужності. LWCRYPT сприяє безпеці розумних об'єктів мереж IoT завдяки своїй ефективній функціональності та невеликім кроком.

Висновки до розділу 2.

IOT - це технологія нової ери, тому проблема захисту та безпеки особливо актуальна. Хоча всі аспекти безпеки не є новими, все ж через зміну платформи та підключення, споживання енергії, використання обмежених ресурсів, довіру до підключених об'єктів з обмеженою перевіркою авторизації та автентифікації змінює сферу захисту, а також способи захисту.

Застосування комп'ютерної техніки для вирішення різноманітних завдань по зберіганню, обробці і передачі інформації призводить до того, що частина завдань з перехоплення даних лежить в площині забезпечення комп'ютерної безпеки. Метою зловмисників стають процеси, пов'язані в тій чи іншій мірі з використанням комп'ютерного обладнання для роботи з інформацією. При цьому піддаються впливу всі складові цього процесу:

Криптографія відкриває нові можливості для підключення до мережі з менш ресурсними пристроями. LWCRYPT [21] працює краще для безпеки IOT у порівнянні з іншими методами завдяки своїй ефективності.

3 АНАЛІЗ ПРОЕКТУВАННЯ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЙНОЇ МЕРЕЖІ

3.1 Проектування персональної інформаційної мережі

Побудова добре захищеної локальної мережі вимагає проектування топології мережі перед тим, як прийняти рішення про те, які фізичні пристрої слід придбати або технології для розгортання. Проект топології визначається як ідентифікація мереж та їх точок взаємозв’язку, розмір і сфера дії мережі, а також тип використовуваних пристроїв взаємозв’язку.

В основному проектування мережі - це одна з чотирьох фаз життєвого циклу PDIOO (Plan Design Implement Operate Optimize - Проектування,Впровадження, Експлуатація, Оптимізація). На цій фазі життєвого циклу мережі завданням проектувальника буде розробка фізичного та логічного дизайну мережевого проекту. Фізичний дизайн мережі пов'язаний з ідентифікацією технологій LAN та WAN та мережевих пристроїв, які повинні реалізувати ефективність логічного проектування в цілому. На цьому етапі розробник мережі відповідає за вибір таких пристроїв, як кабельні проводи, комутатори, мости, маршрутизатори, безпроводова точка доступу та інші. Тобто логічний етап проектування є основою для фізичного проектування мережі, і саме тут розробляють ієрархічну та модульну мережу. Цей етап включає проектування адресації мережевого рівня, вибір протоколів комутації та маршрутизації, планування безпеки та дизайн мережевого управління. Також складність топології залежить від розміру мережі та характеристик трафіку системи.

Персональна інформаційна мережа житлового будинку - це локальна комп'ютерна мережа, що має вихід в Інтернет. По суті, вона нічим не відрізняється від офісних, локальних обчислювальних мереж. Різниця в тому, що до домашніх мереж підключено особисті комп'ютери користувачів, що знаходяться в приватних квартирах.

Поштовхом до розробки таких мереж послугували, з одного боку, бажання користувачів отримувати доступ до нових інформаційних ресурсів, а з іншого - незадоволення якості доступу до Інтернету на комунікативній лінії та відносно високої вартості доступу.

Підключившись до персональної мережі житлового будинку, абонент отримує можливість користуватися різними видами сервісу. У залежності від конкретного провайдера це може бути:

- доступ до власного інформаційного сервера мережі;
- послуги IP-телефонії;
- можливість організації віртуального офісу.

Одним з основних аргументів у використанні таких мереж є універсальність застосованих технологій: з їх допомогою можна запропонувати абонентам широкий спектр послуг [5].

3.1.1 Концепція побудови мережі

В якості базової топології можуть бути використані схеми, характерні як для міських, так і для корпоративних мереж. Дуже часто мережа житлового будинку не обмежується територією однієї будівлі, а охоплює цілий мікрорайон. Тому на практиці її топологія нагадує зменшену копію мережі міського класу. Топологія, типова для корпоративних мереж, найчастіше застосовується для підключення локально згрупованих абонентів - наприклад, що живуть в одному під'їзді.

У будь-якому проекті побудови такої мережі можна виділити ряд обов'язкових компонентів (рис 3.1):

- Вузол агрегації трафіку, через який мережа житлового будинку підключається до опорної міської мережі. У вузлі агрегації трафіку розташовуються внутрішні інформаційні сервера мережі і підключається магістральний канал від провайдера послуг.
- Точки доступу, що знаходяться в кожному будинку і з'єднані з вузлом агрегації трафіку. До точкам доступу по кабельній інфраструктурі підключаються особисті комп'ютери користувачів. Залежно від числа абонентів, в будинку може бути встановлено кілька точок доступу. Основним критерієм є висока масштабованість як за кількістю підключення користувачів, так і за пропускною здатністю.
- Клієнтське обладнання. Як правило, це мережева карта з інтерфейсом Ethernet. Також можливе використання некерованих комутаторів, якщо замовнику необхідно підключити більше одного комп'ютера.
- Системи білінгу для управління обліковими записами абонентів, політикою доступу і тарифними розрахунками.

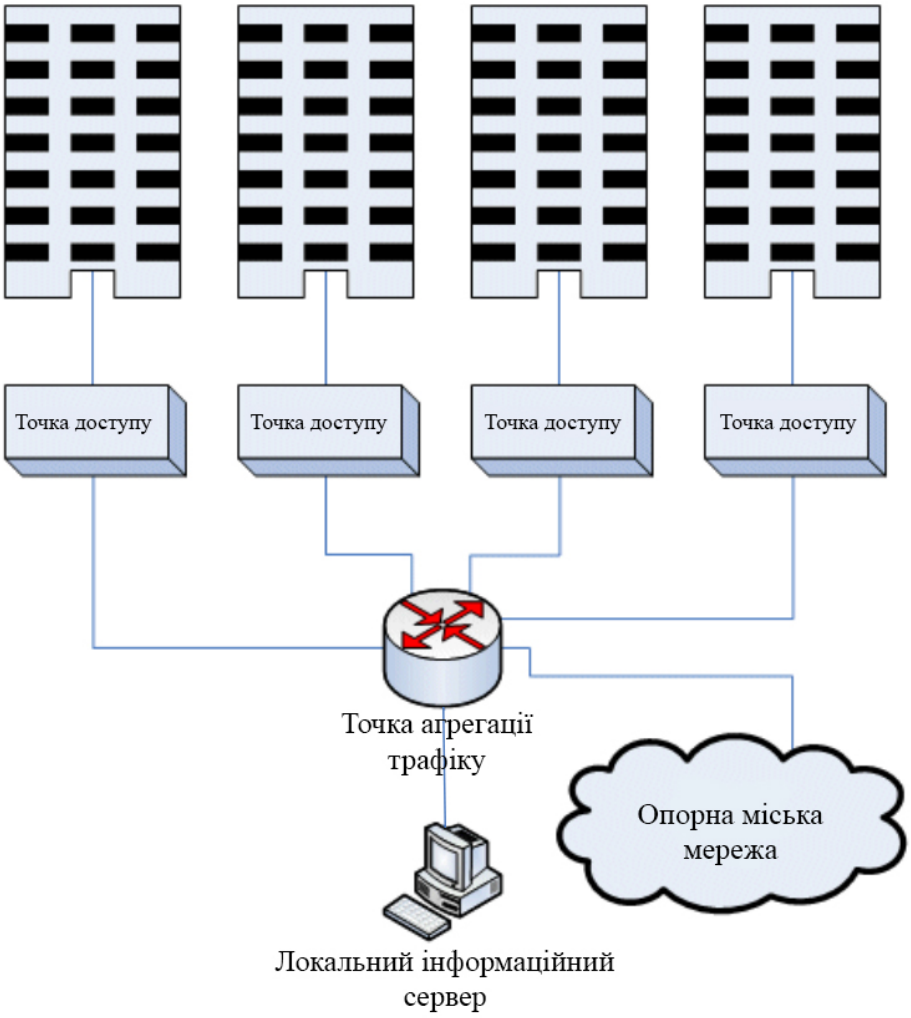


Рисунок 3.1 – Топологія локальної інформаційної мережі житлового будинку

3.1.2 Технології та обладнання для мережі житлового будинку

Найбільш популярними технологіями для побудови мережі житлового будинку є Home PNA, Passive Optical Network (PON), Ethernet [5].

Технологія Home PNA була розроблена в 1998 році альянсом виробників телекомунікаційного обладнання. Залежно від якості ліній, пікова швидкість передачі за технологією Home PNA може досягати до 32 Мбіт / с, а пропускна здатність каналів зв'язку - 20 Мбіт / с. Чудова властивість Home PNA - повна спектральна сумісність з традиційною телефонним зв'язком і обладнанням DSL-ліній, так як для передачі сигналів в ній відведено діапазон частот від 4 до 10 МГц. Зворотною стороною такого зручності є мала максимальна відстань (всього 350 м), на яку можуть бути рознесені вузли мережі. Крім того, в одній мережі Home PNA [16-18] забезпечується

підтримка не більше 25 вузлів. У точці доступу встановлюється маршрутизатор Home PNA або звичайний міст з інтерфейсом Ethernet, за допомогою якого здійснюється підключення до міської мережі. У комп'ютери користувачів вставляються адаптери Home PNA, що з'єднуються по мідній лінії з обладнанням в точці доступу. В якості мідної проводки можна використовувати існуючу розводку телефонної мережі, але краще протягнути альтернативний кабель. На відміну від стандартної технології Ethernet по витій парі, де до кожного клієнта доходить власний кабель, технологія Home PNA дозволяє робити відводи від загального кабелю.

В основі технології PON лежить поділ потоків даних за різними оптичними довжинами хвиль ("несучими"). Сучасне покоління обладнання PON забезпечує підключення до 32 термінальних вузлів при протяжності оптичного сегмента не більше 20 км. Пасивна оптична мережа оптимально підходить для створення канальної інфраструктури, що з'єднує точки доступу в мережі житлового будинку. Завдяки цьому оптимізуються і здешевлюються витрати на кабельні траси між будівлями, так як PON підтримує топологію дерево, а бічні відводи робляться за допомогою сплітерів, що не вимагають електроживлення. Більш того, при виході з ладу однієї з ділянок мережі це ніяк не позначається на працездатності. Основним недоліком є висока вартість абонентського обладнання: дана технологія частіше використовується для підключення корпоративних клієнтів.

При розгортанні кабельної інфраструктури провайдери використовують в якості середовища передачі Ethernet стандартний кабель - виту пару. При цьому абоненту надається канал даних на швидкостях 10/100/1000 Мбіт/с, а відстань від активного мережного обладнання до комп'ютера абонента не повинна перевищувати 100 метрів. Для збільшення відстані використовується каскадне включення активного обладнання. Найдешевшим варіантом вважається застосування некерованих концентраторів Ethernet, але в цьому випадку всі абоненти знаходяться в єдиному мережевому сегменті і змушені "конкурувати" за пропускну здатність загального середовища доступу. Для вирішення цієї проблеми рекомендується використовувати керовані комутатори 3-го рівня з більшою щільністю портів і підтримкою механізмів QoS [5].

3.2 Огляд мережевої безпеки

Ще з давніх часів люди охороняють свою власність. Відсутність охорони може спричинити втрату майна чи життя людини. З плином часу стала актуальною проблема захисту інформаційної та цифрової власності. Подібним чином комп'ютерні ресурси повинні бути захищені від внутрішніх і зовнішніх зловмисників. Єдиний спосіб забезпечення повної комп'ютерної безпеки - це обмеження будь-якого фізичного та логічного доступу до системи. Очевидно, що повне розділення комп’ютерів один від одного створює безпечну зону; проте так втрачається передача даних, що робить систему марною.

Як відомо, комп’ютер є більш корисним, коли він є частиною мережевої системи. Мережеве середовище допомагає збільшити продуктивність праці, а також створити сприятливе середовище для конкуренції компанії на світовій арені. Однак важливо вжити певних заходів безпеки, щоб зменшити або, якщо можливо, уникнути ризиків безпеки, спричинених несанкціонованим доступом до системних ресурсів та послуг, що загрожує продуктивності і цілісності компанії [5].

Компанії невтомно працюють, щоб максимізувати свій прибуток. Для цього вони використовують найшвидші способи спілкування. Сьогодні Інтернет є найдешевшим, найшвидшим та найпростішим засобом спілкування для ведення бізнесу на глобальному рівні. Інтернет змінив спосіб життя та роботи людей і навіть змінив спосіб ведення бізнесу. Окрім можливостей, Інтернет втрачає компонент безпеки, а отже, локальна мережа без заходів безпеки має великий ризик втратити ресурси та інформацію.

Отже, сьогодні компаніям потрібно застосовувати ефективні заходи безпеки для захисту своїх цінних мережевих ресурсів від атак. На цьому етапі варто визначити, що таке безпека мережі. Згідно Cisco отримано наступне визначення [13-15]:

«Безпека мережі включає виявлення та запобігання несанкціонованому доступу як до елементів мережі, так і до пристроїв, підключених до мережі. Сюди входить все: від запобігання несанкціонованому доступу до порту комутатора до виявлення та запобігання несанкціонованого мережевого трафіка як усередині корпоративної мережі, так і за її межами ».

Основною причиною впровадження мережевої безпеки є захист мережі та системних ресурсів, підключених до мережі. Інформація в будь-якій формі вважається цінною властивістю мережі, і її втрата чи доступ до неї може коштувати грошей або в гіршому випадку, спричинить катастрофу.

Впровадження засобів контролю безпеки в мережевому середовищі дозволяє мережевій системі працювати належним чином. Через це компанії, уряди та інші організації надали пріоритет безпеці мережі та витратили мільярди на планування та впровадження нових технологій захисту.

У сучасних відкритих умовах організаціям, які хочуть надати загальнодоступний доступ до мережевих ресурсів, потрібно проаналізувати загрози безпеки, які можуть призвести до нападу на систему. На цьому етапі варто нагадати, що атака може статися зсередини приміщення мережі і з боку довірених працівників.

3.2.1 Вразливості системи

Вразливість - це характеристика комп'ютера або мережевої системи, яка створює слабкі місця в загальній системі безпеки комп'ютера або мережі, яка може бути використана для атаки мережі. Для атаки мережі зловмисники використовують ненадійність вразливості, щоб завдати потенційної шкоди комп'ютеру або мережевій системі.

В основному, вразливість системи можна простежити за трьома основними джерелами: відсутність ефективної політики безпеки мережі, слабкі місця в конфігурації мережі та технологічні недоліки.

Відсутність ефективного механізму безпеки мережі. Організація чи то компанія повинна мати письмовий документ, в якому чітко вказується, що робити щодо питань безпеки, які мають найбільше значення, щоб підтримувати діяльність організації. Якщо політика характеризується відсутністю однакових дій в застосуванні певних механізмів забезпечення, відсутністю плану аварійного відновлення, відсутності корегування помилок та вразливостей, відсутності моніторингу журналів та відсутності належного контролю доступу, це створить прогалини в безпеці та зробить мережу більш вразливою до атак.

Слабкі сторони конфігурації мережі. Люди схильні до тих чи інших помилок. Вразливості конфігурації - це людський фактор, спричинений відсутністю знань або нерозумінням. Такі вразливості трапляються, коли використовуються слабкий пароль, неправильно налаштовані мережеві пристрої, неправильно налаштовані Інтернет-послуги (HTTP, FTP, Telnet тощо) та налаштування за замовчуванням. Кожен з них надає чудову можливість для хакерів зловживати мережевими ресурсами. Однак можна

запобігти пошкодженню заздалегідь, застосовуючи стандартні базові конфігурації.

Слабкі сторони технологій. Нинішні технології не є ідеальними для надання необхідних продуктів та послуг без прогалин у безпеці. Майже все апаратне обладнання, програмні продукти (операційні системи та додатки), протоколи (TCP/IP та протоколи маршрутизації) мають дефекти, які можуть призвести до вразливості системи та зробити системи, яким вони належать, схильними до атак.

3.2.2 Загрози

Загроза - це все, що можна вважати потенційною причиною події, яка здатна використати вразливість мережевої системи, щоб завдати шкоди організації, порушуючи спроектовану роботу мережі. Загроза може бути ініційована навмисно людьми або випадково внаслідок несправність комп'ютерів та системних компонентів.

Як правило, загрози групуються у дві великі категорії: структуровані загрози та неструктуровані загрози. Перший тип загроз є найскладнішим для добре організованої мережі щодо спроби нападу на цільову систему. В основному, зловмисники висококваліфіковані і здатні маніпулювати вразливостями системи для власної вигоди. Останній тип загроз є найбільш випадковими і ініціюються будь-якою особою, яка виявляє вразливості системи за допомогою інструментів сканування, які є у вільному доступі в Інтернеті. Наприклад, існують безкоштовні програми для скриптів і зломщики паролів, які використовуються зловмисниками, або встановлення пароля для доступу до системи для пошуку будь-якої інформації. Незважаючи на те, що напади не організовані, як попередні, вони все одно здатні завдати серйозної шкоди.

3.2.3 Атаки

Згідно з робочою групою Інтернет інженерії (Internet Engineering Task Force - IETF), «атака - це посягання на безпеку системи, яка походить від інтелектуальної загрози, тобто розумного акту, який є навмисною спробою ухилення від служб безпеки та порушує політику безпеки системи ". Атака може бути будь-якою спробою дізнатись або зібрати інформацію, не

впливаючи на системні ресурси (пасивна атака, наприклад, збір інформації про пакети), або може бути серйозною, спрямованою на маніпуляції з ресурсами та порушення роботи системи (активна атака, яка включає відмову в обслуговуванні). Така атака ініціюється або з внутрішніх периметрів безпеки, які є довіреними об'єктами (внутрішня атака), або з зовнішніх периметрів безпеки, які не мають дозволу на доступ до системи (зовнішня атака).

Технічно кажучи, щодо цілей, які вони досягають, атаки групуються у три основні категорії: розвідувальні атаки, атаки доступу, DoS атаки (відмова в обслуговуванні).

Розвідувальна атака. Розвідувальна атака пов'язана з доступом до системи для будь-якого роду вразливостей для запуску атак на мережеву систему. У цьому випадку втрата відбувається не відразу; однак це створює можливість для хакерів або зловмисників ініціювати цілеспрямовану атаку на мережеву систему. Розвідувальна атака, як правило, спрямована на виявлення інформації про DNS (систему доменних імен) за допомогою запитів пошуку, діапазону підмереж та хостів за допомогою програмного забезпечення Ping sweep, відкритого порту за допомогою сканера портів та вивчення вразливостей пакетів за допомогою пакету спуфінг.

Атака доступу. Такий тип атаки націлений на отримання доступу до системи або мережі без законної автентифікації. Зловмисники використовують різні інструменти для перехоплення трафіку даних та вилучення такої важливої інформації, як пароль, щоб отримати доступ до системи та зловживати мережевими ресурсами, змінити конфігурацію пристрою та додати несанкціонований орган до списку доступу до системи. На додаток до цього, така атака включає введення сфабрикованих об'єктів, які зазвичай здійснюються шляхом зміни вихідних даних, та ін'єкції шкідливого програмного забезпечення.

Комп’ютерна шкідлива програма (включаючи віруси, троянські коні та інші) - це шкідливі програми, призначені спеціально для знищення або пошкодження комп’ютерної системи або мережевих ресурсів. Сьогодні розробник шкідливих програм використовує Інтернет для розповсюдження шкідливих програм, щоб вплинути на якомога більше комп’ютерних систем. Такі програми здатні сповільнювати роботу Інтернету, знищувати файли, впливати на сервери і т. д. Незважаючи на те, що сьогодні існує низка програм шкідливого програмного забезпечення:

- Вірус - це комп’ютерна програма або фрагмент коду, який здатний прикріпитись до хост-програми та дублювати її, коли активується програма-хост. Комп’ютерний вірус як біологічний вірус не саморозмножується. Їй потрібна програма-оператор для розповсюдження з однієї системи в іншу, як вкладення електронної пошти.
- Worm («хробак») - це незалежна програма, що самопоширюється, яка призначена для сканування мережі на наявність уразливості системи, щоб дублювати собі, а потім розповсюджуватись на наступну нову систему.
- Троянський кінь - це програма або фрагменти коду, що ховаються всередині іншої програми, замасковані, щоб користувач сприйняв його як корисні програми, наприклад комерційні ігри. Однак коли програма з троянським конем завантажується, це впливає на систему. Деякі з них здатні змінити чи замінити існуючу програму, створити хакерам «двері», змінити список доступу, а також оновити рівень привілеїв.

Дуже важливо відзначити, що визначення вірусу, «хробака» та троянського коня ускладнюється, зважаючи на їх активний розвиток. Наприклад, розробник комп’ютерних вірусів поєднує в собі ряд функцій вірусів, щоб створити більш стійкий вірус, ніж раніше.

Атаки відмови в обслуговуванні (DoS-атаки). Як випливає з назви, атака на відмову в обслуговуванні - це атака, спрямована на запобігання доступу до послуг тим особам, які мають на це законне право. Система, скомпрометована атакою "Відмова в обслуговуванні", виконує код, який генерує ряд послідовних запитів на послугу для створення "звуження" в лінії передачі даних, і в результаті цього атака робить службу недоступною для законних користувачів . Напад такого типу не вимагає високого рівня майстерності або знань; його може ініціювати особа, яка має базові навички в даній темі. Пінг «смерті», синхронізація замилювання Послідовного Номера (Sequenced Number-SYN), спам є одними з прикладів атак відмови в обслуговуванні.

3.2.4 Аналіз ризиків

Проводячи аналіз ризиків, перш за все важливо зрозуміти основне визначення ризику комп'ютерної безпеки. Ризик безпеки - це ймовірність того, що певна загроза використовує певну вразливість комп'ютерної системи, що призводить до втрат активів та ресурсів. Існує багато різних загроз для мережевої системи, але в аналізі ризиків треба звертати увагу на ті загрози, які мають найбільше значення. На даний момент цифрові журнальні файли є найкращою альтернативою для запуску процесу ідентифікації загроз; деякі з них перелічені нижче:

- Місцева система безпеки встановлення
- Продавці програмного забезпечення
- Місцеві комп’ютерні записи
- Професійна організація комп'ютерної безпеки
- Інформаційний бюлетень та папір про безпеку
- Електронна група новин та список
- Користувачі локальної системи.

Це достатні перелік, щоб охопити загрози, що стоять перед мережевою системою, але ,зрозуміло, потрібно розширити кругозір, щоб також виявити специфічні загрози.

Проведення аналізу ризиків насамперед включає ідентифікацію активів, виявлення ризиків для цих активів та впровадження засобів контролю для зменшення цих ризиків. Це означає, що в процесі дуже важливо знати, які види ризиків існують для ресурсів компанії та як ці ризики можна зменшити або врешті усунути. В основному, показник безпеки в системі повинен бути пропорційним ризикам. Технічно впровадження системи безпеки в комп'ютерну мережу є непростим завданням, і зазвичай такий процес щодо вибору відповідного контролю безпеки є досить суб'єктивним. Первинна ідея проведення аналізу ризиків полягає в тому, щоб поставити ці процеси в об'єктивну основу.

Існує ряд різних підходів до аналізу ризиків. В основному ці підходи групуються у дві категорії: кількісний та якісний аналіз ризиків. Обидва підходи мають свої переваги та недоліки.

3.3 Методи аналізу загроз

3.3.1 Кількісний аналіз ризику

Такий підхід до аналізу ризику, як правило, виражається у грошовій оцінці, і в основному це оціночне значення ймовірності події та збитків, які вона може спричинити. Це очікувана фінансова втрата, з якою компанія стикається в момент виникнення ситуації. Математично кількісні втрати для подій обчислюються щорічно, просто помножуючи потенційні втрати на ймовірність настання даної події. Щоб проілюструвати це, потрібно розглянути практичний приклад. Вважається, що оперативна пам’ять комп’ютера виходить з ладу двічі кожні три роки, а апаратна вартість оперативної пам’яті становить 100 євро. Виходячи з припущень, ймовірність відмови оперативної пам'яті на рік становить 2/3; отже, річна очікувана втрата складе (2/3) * 100 євро, що складає 66,7 євро. [12,4]

Теоретично, можна ранжувати подію на основі розрахованого значення ризику, що в кінцевому підсумку допомагає прийняти рішення про те, яким чином будуть застосовуватися засоби контролю. Однак кількісний аналіз ризику неможливий, коли використовується недостовірні або неточні дані. Наприклад, реалізовані заходи контролю та протидії зазвичай створюють низку потенційних подій, і ці події здебільшого взаємопов’язані між собою. Це ускладнює знання їх під рукою та ускладнює прогнозування ймовірності ймовірності настання події.

3.3.2 Якісний аналіз ризиків

В якісному аналізі ризику не призначається грошова оцінка конкретного ризику, а швидше обчислюються відносні величини для оцінки потенційних збитків. Аналіз проводиться за допомогою анкет та спільних практикумів, в яких беруть участь працівники та власники компанії. Аналітики ризиків розповсюджують анкети для збору інформації про активи компанії, розгорнуті засоби контролю та інші відповідні питання безпеки.

Зібрана інформація корисна для ідентифікації активів та оціночної вартості цих активів. Тобто можна передбачити, з якими загрозами може зіткнутися кожен актив, і уявити, які типи вразливостей ці загрози можуть використати в майбутньому.

3.4 Рішення щодо безпеки мережі

3.4.1 Політика безпеки

Як обговорювалося в розділі 3.2.1, ієрархічний дизайн мережі має три рівні. Перший називається основним шаром; саме тут розташована критична програма та допоміжна система, і її потрібно захищати від зловмисників додатковим рівнем безпеки. Другий рівень називається рівнем розподілу, де розташовані внутрішні користувачі та переважно загальнодоступні ресурси, такі як веб-сервери та FTP-сервери. На розподільчому рівні можна знайти шлюзові програми та мережеві системи (такі як виявлення вторгнень, перевірка вірусів та вмісту), що спеціалізуються на наданні додаткових функцій безпеки, необхідних для захисту системи від сторонніх, а також сторонніх осіб. Третій шар - рівень доступу, де кінцеві користувачі знаходяться для доступу до мережевих ресурсів та послуг, і цей рівень повинен бути захищений від несанкціонованих користувачів. Сьогодні жодна комп’ютерна система не захищена від нападу, і компаніям необхідно застосовувати ефективні заходи безпеки, які здатні захистити їх мережеву систему та ресурси. Щоб протистояти атаці, що надходить зсередини або зовні мережі, адміністраторам компанії потрібно вибрати адекватні технології безпеки та їх розміщення в мережевій системі. Сьогодні доступно безліч технологій безпеки, але вибір та розгортання повинні відповідати загальній меті компанії та політиці безпеки.

Компанії приймають рішення, пов'язані з безпекою, виходячи з власних цілей безпеки, які в основному пов'язані з діловими можливостями, на яких базується їх діяльність. Цілі безпеки компанії повинні бути відомі користувачам та працівникам фірми через набір правил безпеки, який називається політикою безпеки. Відповідно до Запиту на коментарі (RFC) 2196, політика безпеки - це офіційне виклад правил, яких користувачі, яким надається доступ до технологій та інформації організації, повинні дотримуватися. Політика повинна чітко визначати вимоги кожного до захисту технологій та інформаційних активів компанії, а також визначати процедуру виконання вимог.

Перед розробкою політики безпеки необхідно розробити план безпеки, який вирішує, що потрібно захищати і від кого. Найкращий спосіб це зробити, провівши аналіз ризиків, щоб перелічити допустимимі і недопустимі дії. Добре організована політика безпеки включає політику доступу користувачів, політику віддаленого доступу, політику звітності, політика автентифікації, політику обробки випадків, політику доступу до

Інтернету, політику електронної пошти, політику фізичної безпеки, політику обслуговування та політику звітності про порушення.

Як правило, політика не повинна бути надмірно обмежувальною, а спрощувати використання ресурсів з певним рівнем обмежень. Глибина політики безпеки ґрунтується на тому, наскільки ми довіряємо людям, і політика повинна проводити межу між балансом між тим, що дозволяє користувачам отримувати доступ до ресурсів компанії, і повністю відмовляти в доступі до цих ресурсів та активів. Зазвичай мережеві адміністратори разом зі старшими менеджерами компанії відповідають за розробку політики безпеки. Вхідні дані користувачів, співробітників, менеджерів, адміністраторів мережі потребують розробки ефективної політики безпеки.

Оскільки компанії постійно змінюються щодо технологій та напрямків бізнесу, а також ризики для ресурсів та активів компанії змінюються з часом. Отже, документи політики безпеки повинні регулярно переглядатися для забезпечення потреб безпеки. На думку експертів з безпеки Cisco, підтримка безпеки компанії - це нескінченний процес, який ставить її на чотири етапи кругообігу, який називається колесом безпеки. Етапи: впровадження, моніторинг, тестування та вдосконалення.

Після реалізації політики її слід контролювати проти атак, а потім перевіряти відповідні заходи безпеки перед застосуванням вдосконалених заходів безпеки.

Можливо, важливо врахувати винятки з кожного правила, і політика безпеки повинна включати ці винятки, якщо вони існують. Найчастіше системні адміністратори можуть використовувати той самий ідентифікатор користувача, і зазвичай їм потрібно мати право доступу до адміністративних файлів, щоб переглядати файли користувача, коли це необхідно.

3.4.2 Технології безпеки та їх розміщення

Захист протоколу Інтернету (IPsec) - це відкрита стандартна система безпеки, розроблена IETF (Internet Engineering Task Force) для забезпечення безпечного зв'язку через IP-мережі. Це означає, що IPsec пропонує захист протоколів та додатків вищого рівня, що робить його найбільш переважною технологією, що використовується для забезпечення наскрізного зв'язку через мережу IP. В основному, IPsec розроблений для забезпечення конфіденційності, цілісності та автентичності передачі даних та взаємодії пристроїв. IPsec виконує ці завдання за допомогою двох протоколів, які

називаються заголовком автентифікації (AH) та інкапсуляцією корисного навантаження безпеки (ESP), а також стандартними механізмами узгодження та управління ключами.

Заголовок автентифікації (AH) призначений для забезпечення цілісності даних (оригінальної автентифікації) для всієї дейтаграми IP, а отже, він є ефективним заходом проти підробки IP та викрадення сеансів. Інкапсуляція корисного навантаження безпеки (ESP), призначена для забезпечення цілісності та конфіденційності даних шляхом шифрування корисного набору IP-пакетів за допомогою спільного секретного ключа. [15]

На додаток до AH та ESP, набір IPsec містить Internet Key Exchange (IKE), які працюють з протоколом управління ключами Internet Security Association (ISAKMP)/Oakley для управління генерацією та обробкою ключів, а також допомагає створювати асоціації безпеки (SA). Асоціація безпеки - це політика чи правила, узгоджені між одноранговими пристроями щодо того, як між ними відбувається обмін даними. Крім того, IPsec має два режими роботи: тунельний режим і транспортний режим. У тунельному режимі IPsec реалізується між двома шлюзами, а оригінальний пакет IP зашифровується і стає корисним навантаженням нового пакета IP. У транспортному режимі IPsec використовується між хостами, і в цьому випадку вихідна інформація заголовка (джерело та адресат) є незашифрованою, і це робить її видимою для проміжних мережевих пристроїв.

3.4.3 Брандмауер (Firewall)

Брандмауери засновані як на апаратному, так і на програмному забезпеченні, і їх основною функцією є захист комп’ютера або мережевої системи від атак. Тобто апаратний брандмауер - це виділений пристрій зі своєю власною операційною системою на спеціалізованій платформі, тоді як програмний брандмауер - це додаткова програма, завантажена на персональний комп’ютер або на мережевий пристрій, як маршрутизатор для перевірки даних або мережі дорожнього руху. Брандмауер відіграє велику роль у реалізації політики безпеки компанії, і в цьому випадку він вважається системою або групою систем, що використовуються для управління мережевим трафіком на основі правил. Брандмауер використовується як захисний міст, який розмічає внутрішню або надійну мережу на зовнішню ненадійну мережу, таку як Інтернет. Як шлюз контрольної точки, брандмауер

аналізує IP-пакети та приймає рішення про те, чи дозволити прохід на основі попередньо налаштованих правил. Також брандмауер визначає, до якої інформації чи послуг слід отримати доступ ззовні, а також зсередини і ким.

За словами Cisco, брандмауер корисний для перевірки пакетів, реалізації політики безпеки, генерації системи аудиту та повідомлень журналу. Для роботи за бажанням брандмауер використовує один або кілька з наступних технологічних компонентів: фільтрацію пакетів, шлюз рівня додатків (проксі-сервер) та шлюз рівня ланцюга (SOCKS). Кожен з них має різні функції і пояснюється нижче: [13]

- Компоненти фільтрації пакетів допомагають обмежити потік інформації між мережами на основі політики безпеки. Технологія фільтрації пакетів використовує список контролю доступу, щоб дозволити або заборонити трафік, що відповідає правилам, продиктованим політикою безпеки.
- Шлюз рівня програми (проксі-сервер) контролює обмін даними між двома мережами на рівні програми. Це робиться шляхом перевірки пакету даних на вищому рівні шарів OSI (рівень 4, 5, 6 і 7) для контролю або фільтрації вмісту певної послуги відповідно до політики безпеки.
- Шлюз рівня ланцюга (SOCKS) - це особливий тип шлюзу рівня додатків, який призначений для перевірки як програм TCP / IP, так і UDP без будь-якої додаткової обробки та фільтрації пакетів. SOCKS зазвичай використовується для вихідних з'єднань, тоді як проксі-сервер використовується як для вхідних, так і для вихідних з'єднань.

Для побудови ефективного брандмауера ці компоненти використовуються разом, але залежно від вимог може бути використана одна або кілька комбінацій компонентів. Незважаючи на те, що брандмауер призначений для того, щоб дозволити або заборонити вразливій службі захистити внутрішню мережу від зовнішніх атак, обов'язок адміністратора мережі полягає в тому, щоб перевірити журнали користувачів та сигнали тривоги, породжені брандмауером, та якомога швидше оновити політику безпеки.

3.4.4 Фізична безпека

Фізичний доступ до мережевих об'єктів слід контролювати та захищати, щоб уникнути несанкціонованого доступу, крадіжок, вандалізму та зловживання ресурсами та активами компанії. Тільки персонал повинен мати фізичний доступ до мережевого обладнання для виконання своїх робіт. Зазвичай це виконується так - тримаючи критичне мережеве обладнання за замкненими дверима, яке захищає від стихійних лих, таких як повені, пожежі, шторми та землетруси, а також від людських катастроф, таких як терористи, хакери та конкуренти. У комп'ютерному кабінеті мережеве обладнання повинно бути у стійці, яка прикріплена до підлоги або стіни, а кімната повинна бути обладнана джерелами безперебійного живлення, кондиціонером, пожежною сигналізацією, механізмами пожежогасіння та системами водовідведення.

Висновки до 3 розділу.

Персональна інформаційна мережа житлового будинку - це локальна комп'ютерна мережа, що має вихід в Інтернет. По суті, вона нічим не відрізняється від офісних, локальних обчислювальних мереж. Різниця в тому, що до домашніх мереж підключено особисті комп'ютери користувачів, що знаходяться в приватних квартирах.

Побудова добре захищеної локальної мережі вимагає проектування топології мережі перед тим, як прийняти рішення про те, які фізичні пристрої слід придбати або технології для розгортання. Проект топології визначається як ідентифікація мереж та їх точок взаємозв’язку, розмір і сфера дії мережі, а також тип використовуваних пристроїв взаємозв’язку.

Впровадження засобів контролю безпеки в мережевому середовищі дозволяє мережевій системі працювати належним чином. Основною причиною впровадження мережевої безпеки є захист мережі та системних ресурсів, підключених до мережі. Інформація в будь-якій формі вважається цінною властивістю мережі, і її втрата чи доступ до неї може коштувати грошей або в гіршому випадку, спричинить катастрофу.

4 РОЗРАХУНКОВА ЧАСТИНА

4.1 Вихідні дані локальної інформаційної мережі житлового будинку

Об’єктом дослідження є локально інформаційна мережа житлового будинку. Житловий будинок має 3 поверхи та 21 квартиру, тобто це по 7 квартир на кожному поверсі. Припустимо, що в кожній квартирі є проводові підключення до комп’ютера та безпроводові підключення до смартфонів і гаджетів, тобто кожна квартира має точку підключення до мережі з Wi-Fi. Мережа розрахована на вільний доступ до Інтернету, користування інформаційними порталами, відео перегляду, доступу до ігрових та стрімінгових сервісів (HBO, Netflix тощо). Провайдер послуги до Інтернет наддав блок зовнішніх адрес 192.168.0.0 з маскою на 24 (255.255.255.000), тобто родинна мережа має адресу 192.168.0.0/24. IP-адреса - це унікальний 32-розрядний номер, який використовується для ідентифікації мережевого пристрою в IP-мережі. Кожна IP-адреса складається з двох частин - хосту та мережі. Мережева адреса використовується для ідентифікації мережі або підмережі, де знаходиться пристрій, а адреса хоста допомагає ідентифікувати окремий пристрій.

У цьому проекті головною метою дослідження є опис особливостей створення захищеної персональної інформаційної мережі житлового будинку. Створення захищеної мережі вимагає комплексного підходу. Потрібно забезпечити захищеність пристроїв мешканців будинку від шкідливого програмного устаткування, зовнішніх загроз та обмежити доступ до небезпечного контенту. Планується надати безпеку мережі житлового будинку за допомогою програмно-апаратного комплексу.

4.2 Схема мережі житлового будинку

Схема проекту (показана на рисунку 4.1 нижче) розроблена з урахуванням характеристик та особливостей житлового будинку, пояснює підключення абонентів до мережного обладнання з подальшим доступом до мережі Інтернет.

Утворено дві мережі VLAN – внутрішня, та зовнішня.

Для спрощення опису локальну мережу можна умовно поділити на декілька секцій за принципом роботи. Виходячи з цього, отримуються секції, що пояснюють взаємодію і напрями передавання даних в обидві сторони:

секція абонентського доступу, секція комутації і маршрутизації та програмно-апаратний комплекс для забезпечення захищеності мережі.

Секція абонентського доступу – це абонентські маршрутизатори (маршрутизатор 1-21 на схемі), за допомогою яких користувачі отримують доступ до Інтернету.

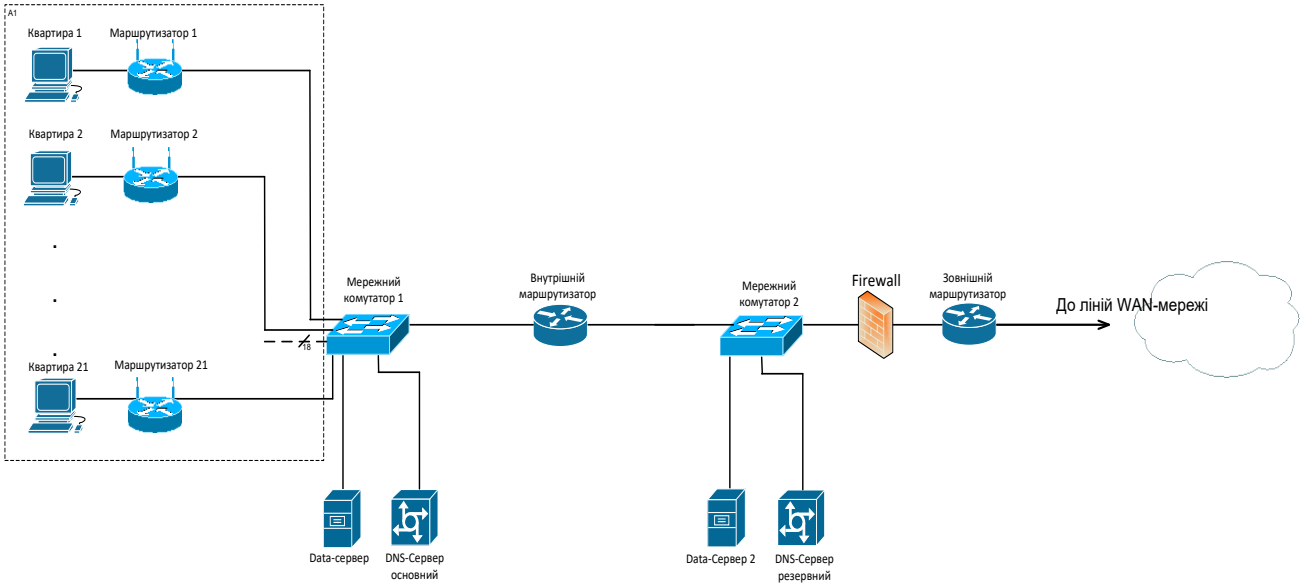


Рисунок 4.1 – Схема локальної інформаційної мережі житлового будинку

Секція комутації і маршршрутизації відповідно складається з двох комутаторів і маршрутизаторів:

- Зовнішній маршрутизатор (Gateway router) – шлюз, знаходиться в будинку, поєднує дві мережі LAN і WAN;
- Мережевий комутатор 2 (access switch) – комутатор рівня доступу;
- Мережевий комутатор 1 (distribution switch) – комутатор рівня розподілу;
- Внутрішній маршрутизатор – шлюз доступу до мережі.

Програмно апаратний комплекс – апаратний комплекс, що забезпечує захист мережі. Він включає в себе файлові сервери (тобто Data-сервер) для зберігання даних доступу до мережі,сховище, в якому зберігаються результати аналізу мережі. В цей комплекс захисту також входить робоча станція з Firewall та іншими програмними налаштуваннями. Детальніше про програмну частину захисту в наступних розділах.

Спрощене зображення локальної інформаційної мережі будинку можна уявити наступним чином:

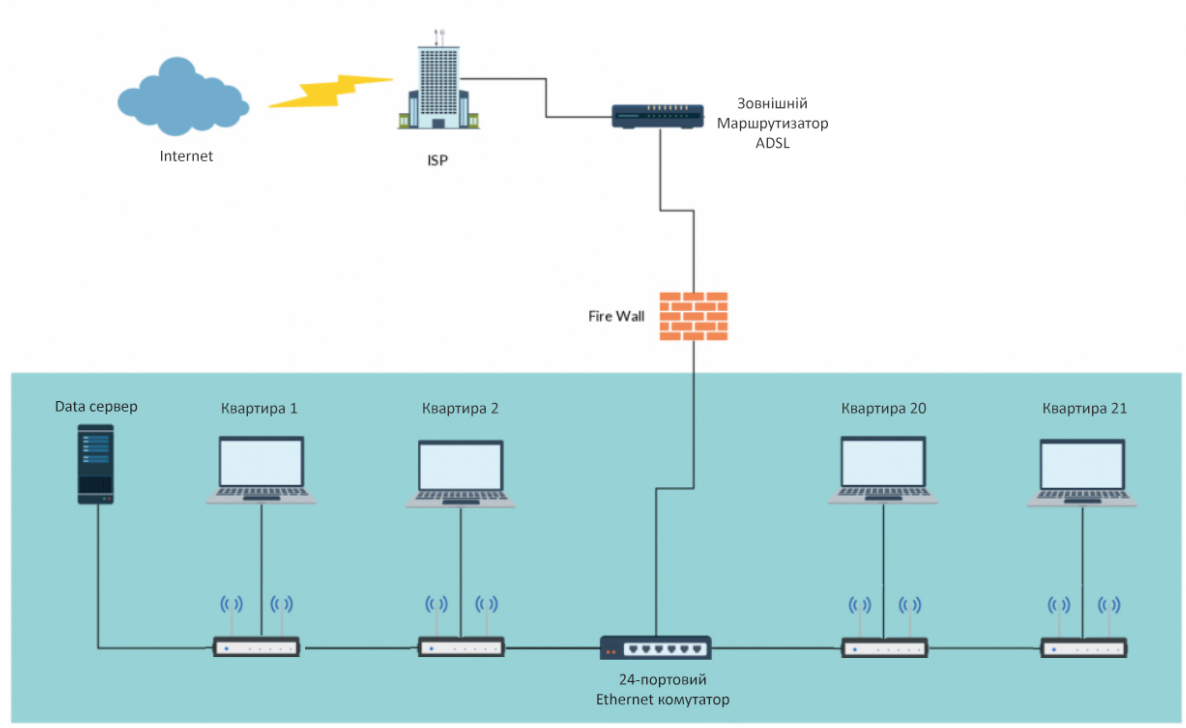


Рисунок 4.2 – Спрощене зображення локальної мережі житлового будинку.

4.3 Забезпечення захищеності локальної мережі житлового будинку

Інструменти захисту повинні створити безпеку абонентського доступу від шкідливого програмного забезпечення, зовнішніх загроз та обмежити доступ до небезпечного контенту. Пропонується забезпечити це наступними програмно апаратними методами:

- Firewall – міжмережевий екран, на вході в мережу для управління доступом до публічної мережі серверів, вхідними та вихідними пакетами даних, запропоновано Cisco (ASA 5505);
- Технологія IDS – на вході мережі після Firewall (немає сенсу контролювати трафік, який буде блокований) для зниження навантаження мережі;
- Snort - утиліта для виявлення вторгнень в мережі (технологія IDS);
- Сканер Assuria Auditor – для сканування рівня вузла;
- Антивірусний захист - це захист, що націлений на абонентські комп’ютери і робочі станції, сервери. Основний рубіж захисту для локальної мережі. Пропонується встановити на усьому обладнанні;
- Захист Wi-Fi мережі в квартирах;
- Фізичний захист обладнання.

4.3.1 Firewall

Спочатку треба встановити, як один з етапів програмного налаштування мережі, програмне забезпечення на комп’ютерах серверів в локальній мережі. Нехай на серверних комп’ютерах встановлено операційну систему Windows 7.

В операційній системі Windows є вбудований мережевий фільтр, проте пропонується посилити захист і встановити Firewall перед мережевими комутаторами.

Firewall (міжмережевий екран, брандмауер) - програмний елемент комп'ютерної мережі, що здійснює контроль і фільтрацію проходить через нього мережевого трафіку відповідно до заданих правил [26].

За допомогою межсетевого екрану прямо з панелі управління комп’ютера можна керувати доступом до публічної мережі серверів, що вхідними та вихідними пакетами даних. Данна опція окремо не тарифікується і входить у вартість мережі.

Для уникнення конфлікту правил мережевого екрану та його правильної настройки необхідно розуміти порядок дій діючих брандмауерів. Можна налаштувати firewall для приватної мережі, для сервера через панель управління, наприклад, для Linux через iptables, для Windows - вбудований.

Для вхідних пакетів першим буде застосовано мережевий фільтр на рівні мережі (за наявності). Якщо пакет пройшов, далі буде застосовано firewall на рівні сервера, в останню чергу буде використаний внутрішній програмний механізм. Для вихідних пакетів буде застосовано зворотню послідовність дій.

Є два типи мережевих екранів: host-based і network. Як зрозуміло з назви, host-based встановлюється саме на абонентський комп’ютер та захищає саме цей комп’ютер. Це може бути корисно в домашніх умовах (особливо, якщо є один комп'ютер і він підключений до модему) або в окремому оточенні, як додатковий засіб безпеки.

Network firewall захищає всю мережу і зазвичай служить шлюзом для цієї мережі. Мережа може складатися як з одного комп'ютера, так і з багатьох тисяч. Тип брандмауера - це вибір у залежності від середовища та потреб.

Мережевий брандмауер поділяється на 2 види: на базі ПК (заснований на звичайному комп'ютері) та ASIC-accelerated. ASIC (application-specific integrated circuit) - мають на увазі машини, в яких основна функціональність брандмауера відбувається на апаратному рівні. Як правило, це дуже дорогі системи, вартість яких доходить до кількох десятків і навіть сотень тисяч доларів. Зазвичай використовуються в ISP-подібних організаціях, яким потрібна дуже висока пропускна здатність.

Для досліджуваної мережі житлового будинку підходить саме Network firewall. В якості брандмауера запропоновано адаптивний пристрій безпеки Cisco (ASA 5505) для захисту від атак, що надходить із зовнішньої мережі на внутрішню мережу. ASA 5505 - це повнофункціональний пристрій безпеки, здатний запропонувати високопродуктивний брандмауер, SSL та IPsec VPN, а також багато інших мережевих послуг для мереж малих та середніх компаній. ASA 5505 має гнучкий восьмипортовий перемикач швидкого Ethernet 10/100 і здатний підтримувати до трьох VLAN. [15,72]. В модельованій мережі цього проекту було створено дві VLAN: внутрішню та зовнішню VLAN. Внутрішня VLAN - це мережа, призначена внутрішній мережі, а зовнішня VLAN - це зона шлюзу, тобто підключення доWAN мережі. Обидві мережі підключені ASA 5505 брандмауеру.

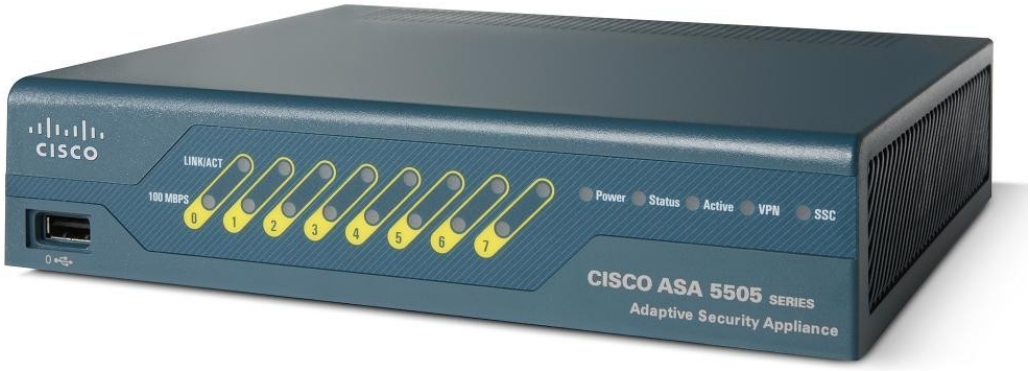


Рисунок 4.3 – Міжмережевий екран Cisco ASA 5505

В основному кожному інтерфейсу ASA 5505 потрібно призначити рівень безпеки від 0 до 100. Внутрішньому інтерфейсу присвоєно рівень безпеки 100, а зовнішньому - 70. Рівень безпеки визначає пріоритети наступних мережевих трафіків, застосовуючи неявний дозвіл від інтерфейсу вищої безпеки до інтерфейсу нижчої безпеки. Це означає, що хост з

інтерфейсу вищого рівня безпеки може отримати доступ до будь-якого хосту на інтерфейсі нижчого рівня безпеки, але не навпаки.

4.3.2 Технологія IDS та встановлення утиліти Snort

Задача IDS (Intrusion Detection System) полягає у виявленні та реєстрації атак, а також сповіщення при спрацьовуванні певного правила. Залежно від типу, IDS вміють виявляти різні види мережевих атак, виявляти спроби несанкціонованого доступу або підвищення привілеїв, появу шкідливого ПО, відстежувати відкриття нового порту і т. д. На відміну від брандмауера, який контролює тільки параметри сесії (IP, номер порту і стан зв'язків), IDS «заглядає» всередину пакета (до сьомого рівня OSI), аналізуючи дані, що передаються. Існує кілька видів систем виявлення вторгнень. Досить популярні APIDS (Application protocol-based IDS), які моніторять обмежений список прикладних протоколів на предмет специфічних атак. Типовими представниками цього класу є PHPIDS, що аналізує запити до PHP-додатків, Mod_Security, що захищає веб-сервер (Apache), і GreenSQL-FW, блокуючий небезпечні SQL-команди.

Для реалізації IDS пропонується встановити на сервер 2 утиліту Snort після Firewall (немає сенсу контролювати трафік, який буде блокований) для зниження навантаження мережі.

Snort - утиліта для виявлення вторгнень в мережі (IDS - Intrusion Detection System). Вона сумісна з ОС Windows і Linux. Всі виявлені загрози (список параметрів подачі тривоги має тонкі настройки), записуються в лог-файл. Snort працює за принципом аналізу пакетів транспортного рівня, тому для його використання, потрібен переклад мережевої карти в спеціальний моніторний режим. Розробники враховували проблему споживання системних ресурсів системами класу IDS, тому Snort невимоглива до апаратного забезпечення і працює у фоновому режимі. Snort не має графічної оболонки (GUI), в зв'язку з чим будь-яка робота з програмою можлива тільки за допомогою командного рядка.

Перший крок – завантаження та установка утиліти Snort.

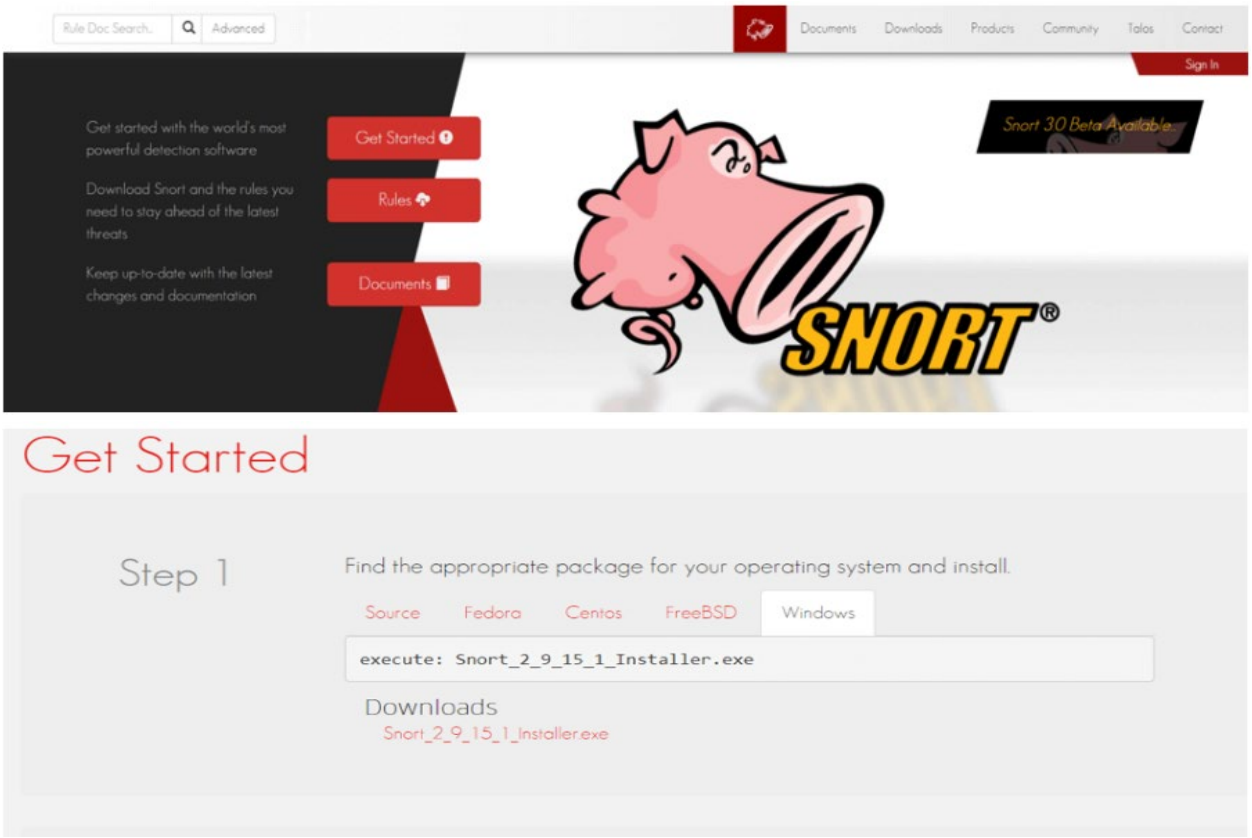


Рисунок 4.4,4.5 – Установка утиліти Snort.

Після установки Snort ніяких змін на комп'ютері не відбулося і працювати з програмою немає можливості, тому що не встановлені спеціальні утиліти і драйвера, які забезпечать запуск програми.

У завершальному вікні Snort для Windows дає запит на встановлення утиліти Winpcap. Це драйвер, який дозволить мережевої карті комп’ютера перейти в моніторний режим, тобто передавати і отримувати пакети, обходячи стеки протоколів. Дана утиліта теж безкоштовна, тому її можна завантажити з сайту розробника www.winpcap.org.

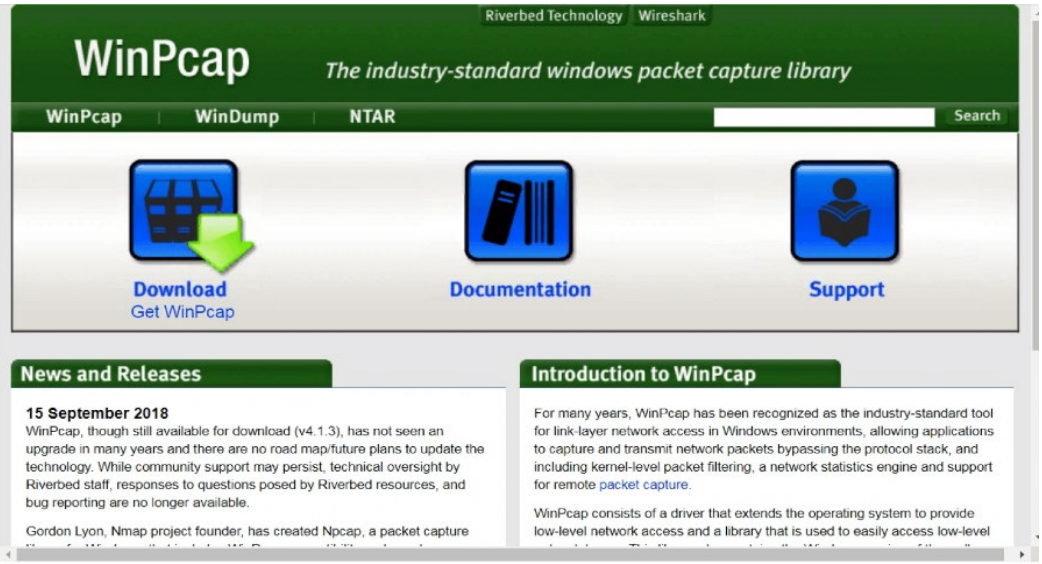


Рисунок 4.6 – вікно завантаження драйверу Winpcap.

Оскільки графічної оболонки для утиліти Snort немає, треба завантажити спеціальні правила, за якими Snort буде працювати. На офіційному сайті Snort.org потрібно взяти список правил (rules), відповідний встановленій версії (вони розсортовані за версіями Snort, а не по операційним системам). На початок 2020 року для Windows актуальна версія 2.9.15.1

Потрібно відкрити файл snort.conf (параметри конфігурації для запуску додатку) в NotePad++.

```
177 # config bpf_file:
178 #
179
180 # Configure default log direc
181 #
182 config logdir: c:\snort\log
```

Рисунок 4.7 – лістинг утиліти snort.

В рядках лістингу вказуємо шлях розташування файлу: c:\snort\rules. Далі вказуємо шлях для папки Log-файлів, куди Snort буде записувати все логи, доступні для перегляду і вивчення:

logdir: c:\snort\log

Наступний крок – потрібно редагувати шляхи для libraries :

path to dynamic preprocessor libraries

dynamicpreprocessor directory c:\Snort\lib\snort_dynamicpreprocessor

path to base preprocessor engine

dynamicengine c:\Snort\lib\snort_dynamicengine\sf_engine.dll

path to dynamic rules libraries

#dynamicdetection directory c:\Snort\lib\snort_dynamicrules

Далі потрібно виправити шляхи правил та визначити мережеву карту карту snort –W. Далі можна запускати режим IDS:

snort -A console -c c:\snort\etc\snort.conf -l c:\snort\log -i 2.

4.3.3 Сканер Assuria Auditor

Сканери рівня вузла краще виконують пошук вразливостей, тому що вони встановлені безпосередньо на вузлі, де потрібно проводити сканування. Вони працюють від імені адміністратора з усіма привілегіями, що також додає можливостей для кращого сканування. З огляду на їх функції, вони можуть здійснювати пошук працюючих на вузлі пристроїв, таких як модеми, а також виявляти встановлені на вузлі додатки або контролювати режим роботи мережевого адаптера . За допомогою сканерів рівня вузла доцільно виконувати ті перевірки, які неможливі або важко виконати для мережевих сканерів або займають багато часу.

Локальні агенти, що запускаються безпосередньо на об'єкті перевірки, забезпечують високу достовірність результатів, оскільки мають повний доступ до файлової системи, реєстру і іншим необхідним компонентам. Їх можна поділити на два типи: постійні і тимчасові.

Постійні агенти являють собою повноцінне встановлене на об'єкті перевірки програмне забезпечення. Сканування проводиться періодично. Раніше такий підхід сканування був дуже популярний, зараз він використовується рідко. З використовуваних сьогодні систем такого типу можна навести Assuria Auditor [32]. Саме цей сканер був вибраний для запропонованої локальної мережі житлового будинку.

Рисунок 4.8 – Домашня сторінка програми Assuria Auditor

Пропонується встановити цей додаток на кожному сервері (їх два).

Детальніше про мережевий сканер Assuria Auditor [32]: це служба, що працює від імені облікового запису «local system», вона завантажується при запуску комп'ютера і працює у фоновому режимі, сканування запускається по команді з консолі. Результати сканування зберігаються за заданим шляхом.

Основними особливостями інформаційного менеджера Assuria Auditor є:

• Огляд всіх налаштованих системних змін, виправлень, користувачів/груп, пакетів та стандартів.

• Вбудований засіб пошуку для швидкого пошуку ключових даних.

• Вбудована звітність для кожного перегляду.

• Інтеграція з базою даних Assuria Auditor Console.

• Швидке визначення ключової інформації.

• Швидкий доступ до деталей цих змін.

• Експорт у Excel/буфер обміну. Вставка в Блокнот для невеликого швидкого звіту.

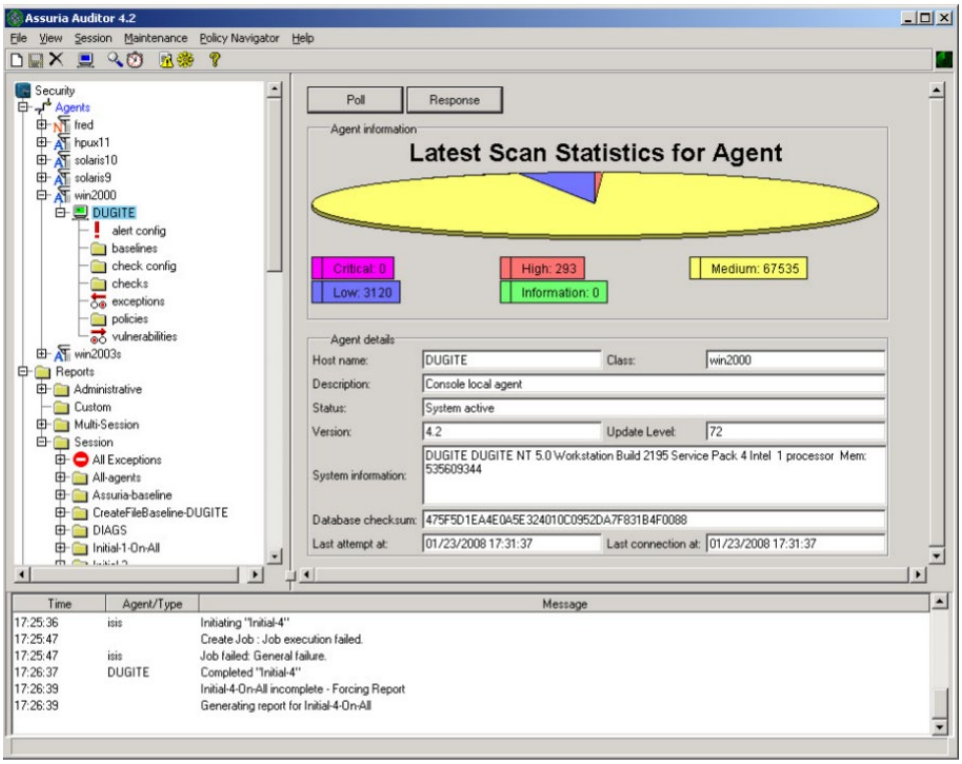


Рисунок 4.9 – Менеджер інформації Assuria Auditor

Окрім перевірок на відповідність нормативним вимогам та стандартам, Assuria Auditor надає набір перевірок відповідності, які є особливою формою

файлу Check Config, що дозволяє налаштувати Assuria Auditor [32] на виконання вимог політики безпеки до дуже конкретного рівня. Перевірка відповідності - це перевірка, в якій використовуються файли Check Config, призначені для модифікації користувачами. Файли Check Config використовуються Assuria для "точної настройки" дій різних перевірок. Файли Assuria Auditor Check Configuration (Check Config) забезпечують дуже потужний механізм налаштування перевірок відповідно до ваших точних вимог. Файли Check Config містять інформацію, на яку посилаються перевірки та політики. Файли Assuria Auditor Check Configuration (Check Config) забезпечують дуже потужний механізм налаштування перевірок відповідно до ваших точних вимог. Файли Check Config містять інформацію, на яку посилаються перевірки та політики. Файли Check Config можна оновити для кожного агента з консолі. Це означає, що ви можете налаштувати їх вміст для кожного агента з одного місця або для всіх агентів або агентів у класі.

Кожна перевірка відповідності має пов'язаний файл конфігурації, який дозволяє налаштувати перевірку. Нижче наведено кілька прикладів файлів конфігурації перевірки відповідності:

• Ключі antiVirus: Цей файл дозволяє вказати, яке антивірусне програмне забезпечення слід встановлювати на комп’ютері. Assuria Auditor використовує вміст цього файлу, щоб переконатися, що на комп'ютері встановлено принаймні один із зазначених антивірусних продуктів.

• Шаблон аудиту: він містить специфікації необхідної політики аудиту сканованої системи.

• UserTemplate: шаблон User дозволяє вказувати конфігурацію користувача.

• Шаблон виправлення: Шаблон виправлення містить специфікації виправлень, які слід застосувати до сканованої системи.

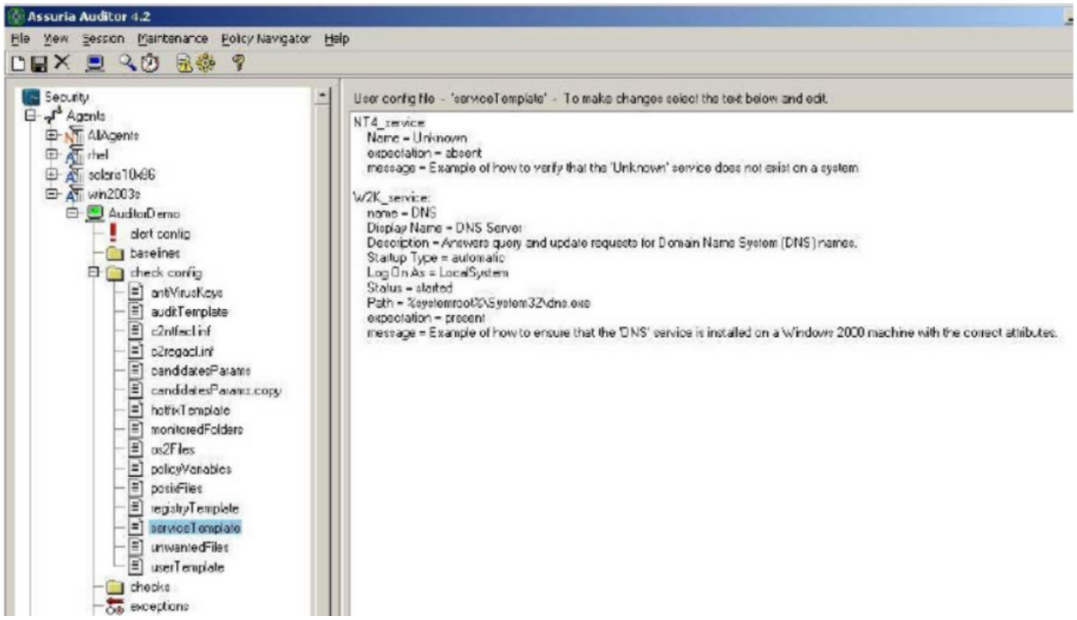


Рисунок 4.10 – Перевірка файлів конфігурації

4.3.4 Антивірусний захист

Антивірусне програмне забезпечення є основним блоком захисту для більшості сучасних мереж і підприємств [31,33].

Насамперед антивірусний захист націлений на абонентські пристрої та робочі станції. Бізнес-версії антивірусів включають функції централізованого управління для передачі оновлення антивірусних баз клієнтських пристроїв, а також можливість централізованого налаштування політики безпеки. В асортименті антивірусних компаній представлені спеціалізовані рішення для серверів.

Враховуючи те, що більшість заражень з шкідливого програмного забезпечення відбувається в результаті дій користувача, антивірусні пакети пропонують комплексні варіанти захисту. Наприклад, захист програм електронної пошти, чатів, перевірка відвідуваних користувачем сайтів. Крім того, антивірусні пакети все більше включають у себе програмний брендмауер, механізми проактивного захисту, а також механізми фільтрації спаму.

Пропонується встановити безкоштовний антивірус Microsoft Security Essential.

Microsoft Security Essentials - безкоштовний антивірус, дає можливість налаштовувати параметри сканування, забезпечує безперервний захист в реальному часі.

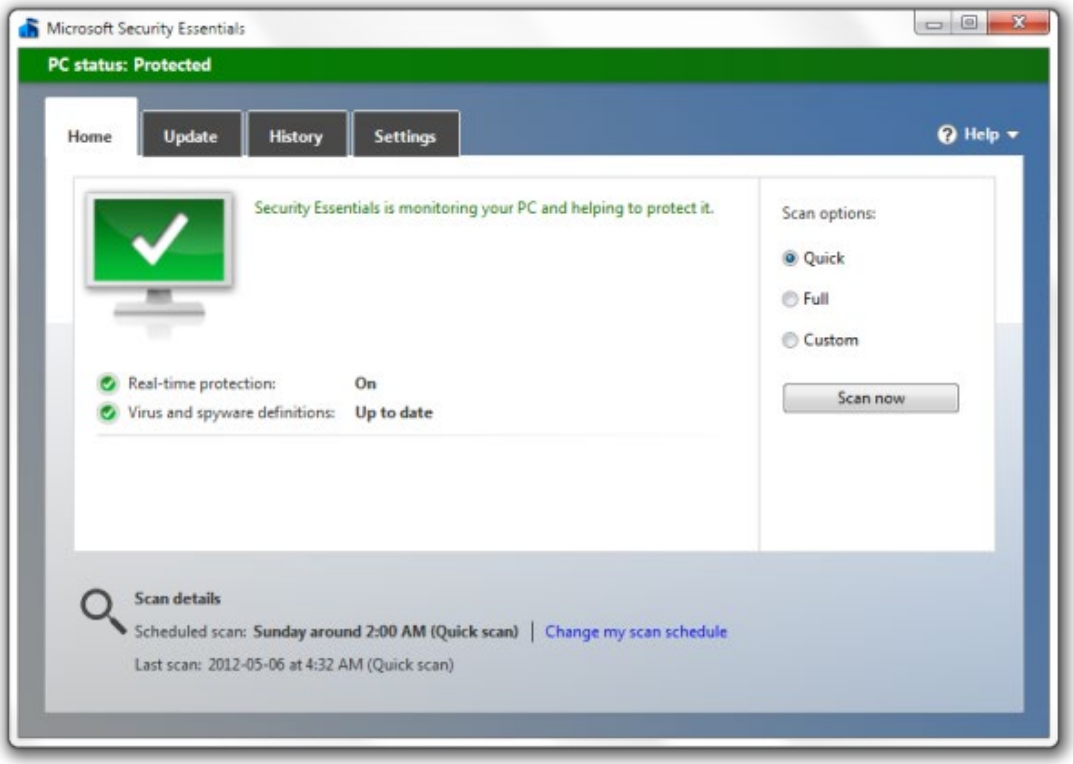


Рисунок 4.11 – вікно Microsoft Security Essentials

Можливості Microsoft Security Essentials:

- MSE (Microsoft Security Essentials) працює у фоновому режимі;
- Інтеграція з брандмауером Windows;
- Інструмент аналізу мережевого трафіку;
- Наявність вбудованого планувальника завдань;
- Автоматично оновлює антивірусні бази;
- Приміщення заражених об'єктів в зону карантину;
- Доступна вибіркова або повна перевірка системи;
- Забезпечує захист від шкідливих програм, інтернет-хробаків, троянів, руткітів та інших загроз [31].

Переваги:

- Створення контрольних точок відновлення системи;
- Не потребує попередньої реєстрації;
- Оновлення софта від офіційного сайту компанії Microsoft;
- Забезпечення високої продуктивності комп'ютера;
- Нова версія антивіруса сумісна з ОС Windows 8 і 10 (32-bit, 64-bit);
- Зрозумілий інтерфейс українською мовою, простий у використанні управління;

- Швидке визначення потенційних загроз і видалення шкідливих об'єктів;
- Надійний захист електронної пошти від рекламного і шпигунського (Adware, Spyware) програмного забезпечення [33].

Пропонується проводити повну антивірусну перевірку раз на два місяці, зважаючи на потреби користувачів локальної інформаційної мережі житлового будинку (завантаження файлів з Інтернету, перегляд різних інформаційних порталів, соцмережі і т.д.).

Віруси та інші шкідливі програми часто модернізуються і вдосконалюються зловмисниками. Це нерідко робить їх непомітними. Через це жоден антивірус не може на 100% захистити комп'ютер від шкідливого ПЗ. Для недопущення зараження потрібно дотримуватися обережності при скачуванні файлів, не переходити за сумнівними посиланнями і вчасно виконувати повну перевірку системи антивірусом.

4.3.5 Захист мережі Wi-Fi

Безпеку мережі Вай-Фай найчастіше стає об'єктом атак різних зловмисників. Причина - в кращому випадку користувачі обмежуються зміною пароля WiFi з заводського варіанту на свій власний, проте це лише третина від необхідних дій [31].

Щоб захистити свою Wi-Fi мережу і встановити пароль, необхідно обов'язково вибрати тип безпеки безпроводової мережі і метод шифрування. На сьогоднішній день необхідно використовувати тільки стандарт безпеки WPA2-PSK з шифруванням AES. Зараз, найчастіше, використовується змішаний варіант WPA / WPA2, який не є безпечним з точки зору злому.

WPA/WPA2 - Personal (PSK) - це звичайний спосіб аутентифікації. Коли потрібно задати тільки пароль (ключ) і потім використовувати його для підключення до Wi-Fi мережі. Використовується один пароль для всіх пристроїв. Сам пароль зберігається на пристроях, де його при необхідності можна подивитися, чи змінити.

WPA/WPA2 - Enterprise - більш складний метод, який використовується в основному для захисту бездротових мереж в офісах і різних закладах. Дозволяє забезпечити більш високий рівень захисту. Використовується тільки в тому випадку, коли для авторизації пристроїв встановлений RADIUS-сервер (який видає паролі).

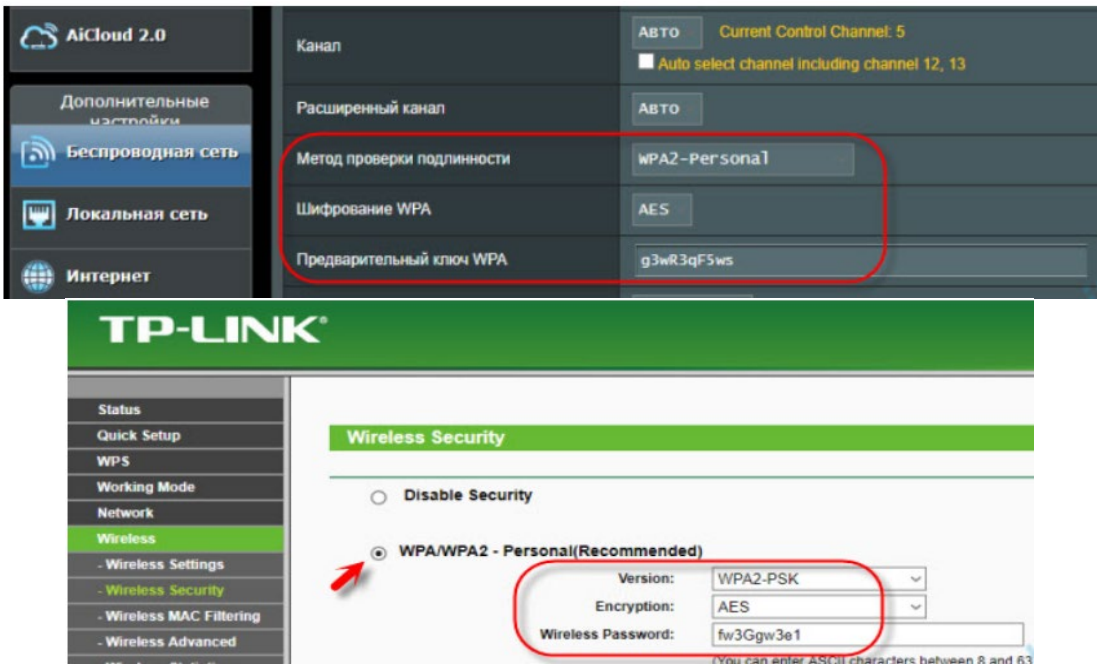


Рисунок 4.12, 4.13 - Настройки захисту безпроводової мережі на маршрутизаторах ASUS(4.12) та TP-Link(4.13)

Наступний крок – встановлення паролю (WPA, Wireless Password). Рекомендується довжину паролю від 8 до 32 символів.

Дуже важливий момент - це технологія WPS (Wi-Fi Protected Setup), яка теж включена на роутері. Це можливість підключитися до мережі без необхідності вводити пароль. Це одна з головних вразливостей, завдяки якій злом WiFi займає небагато часу. Тому пропонується відключити WPS в налаштуваннях безпроводової мережі.

В досліджуваному проекті – квартирний житловий будинок, висока концентрація бездротових мереж, тому не зайвим буде приховати Вай-Фай відключивши трансляцію SSID. Для того, щоб підключити гаджети (смартфони та планшети), потрібно вручну ввести SSID через пункт «Додати мережу» на пристрої.

У тих випадках, коли до абонентського роутера часто підключаються сторонні - друзі, знайомі, клієнти і т.п., то є сенс активувати на роутері ізольовану гостьову мережу. Її клієнти будуть без проблем виходити в Інтернет, але пристрої домашньої мережі бачити не будуть.

Якщо клієнський WiFi маршрутизатор вміє блокувати незареєстровані на ньому пристрою та абонент рідко підключає до нього нові гаджети, то є сенс активувати таку функцію захисту.

На багатьох сучасних модемах і маршрутизаторах є можливість активувати Інтернет-фільтр, який базується на спеціалізованих сервісах типу Яндекс.dns. Після цього велика кількість фішингових сайтів і шкідливих сторінок буде блоковано і досить успішно відфільтровано вже на стадії запиту.

4.3.5.1. Захист абонентського WiFi маршрутизатора

В останні роки все масові зараження і зломи роутерів відбуваються завдяки виявленим вразливостям і помилок в їх прошивці. Яскравий приклад - вірус VPNFilter, який вразив понад 500000 маршрутизаторів в 54 країнах світу. Зараз під загрозою знаходяться пристрої від LinkSys, NetGear, TP-Link і Microtik, але не виключені і інші марки. Єдиний на сьогодні спосіб боротьби - скидання налаштувань і оновлення прошивки роутера.

Пропонується завантажити актуальну версію ПЗ на сайті виробника і встановити цей файл, або на багатьох сучасних мережевих пристроях реалізована функція автоматичного оновлення прошивки. У цьому випадку досить просто натиснути кнопку і дочекатися завершення процесу.

В обов'язковому порядку необхідно змінити пароль адміністратора на доступ до конфігурації пристрою. Деякий час назад по мережі гуляв вірус Trojan.Rbrute, який зламував роутери, на яких використовувався або заводський, або дуже простий пароль, наприклад 1111, qwerty і т.п.

Пароль на доступ до налаштувань бажано робити не менше 8-10 символів довжиною і з цифр і букв різного регістра.

Мало хто зі звичайних абонентів користується доступом до веб-інтерфейсу з Інтернету, тому ж це теж потенційна пролом у захисті маршрутизатора. Тому рекомендується вимкнути цю опцію.

4.3.6 Фізична безпека

Фізична безпека локальної мережі є одним з найважливіших факторів, який складно переоцінити. Маючи фізичний доступ до мережних пристроїв зловмисник, в більшості випадків, легко отримає доступ до мережі. Наприклад, якщо є фізичний доступ до комутатора і в мережі не проводиться фільтрація MAC-адрес. Хоча і фільтрація MAC в цьому випадку не врятує. Ще однією проблемою є крадіжка або недбале ставлення до жорстких дисків після заміни в сервері або іншому пристрої. З огляду на те, що знайдені там

паролі можуть бути розшифровані, серверні шафи і кімнати або ящики з обладнанням повинні бути завжди надійно захищені від проникнення сторонніх.

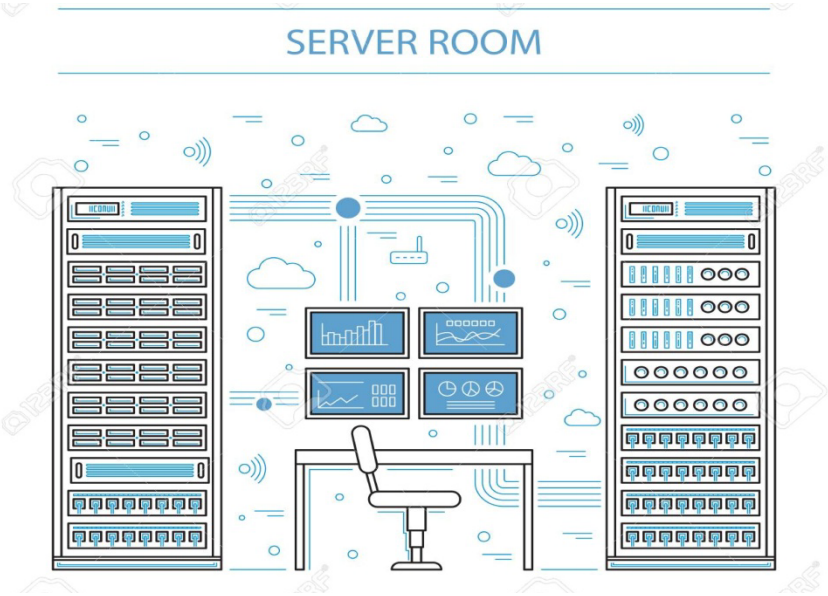


Рисунок 4.14 – Схематичне зображення кімнати з мережевим обладнанням

Пропонується наступне: тримати критичне мережеве обладнання за замкненими дверима, в сухому приміщенні, яке добре вентилюється, де регулярно проводяться сухі прибирання від пилу. Двері захищають від погодних умов, а також від людських факторів, таких як терористи, хакери або конкуренти. У комп'ютерному кабінеті мережеве обладнання повинно бути у стійці, яка прикріплена до підлоги або стіни, а кімната повинна бути обладнана джерелами безперебійного живлення, кондиціонером, пожежною сигналізацією, механізмами пожежогасіння та системами водовідведення.

Висновок до 4 розділу.

В даному розділі наведені програмні та програмно-апаратні можливості захисту для персональної інформаційної мережі житлового будинку. Побудовано графічне зображення топології мережі для кращого візуального сприйняття. Зважаючи на всі особливості та потреби абонентської мережі, запропоновані методи захисту. Всі перераховані методи захисту працюють в комплексі, вони допомагають підтримувати стабільну захищеність мережі кожен на своєму рівні. Проте технології зараз дуже швидко змінюються та ростуть, тому потрібно підтримувати ПЗ в актуальному стані та слідкувати за оновленнями та новими можливостями захисту мережі.

5 СТАРТАП ПРОЕКТ

5.1 Опис ідеї проекту

В даній роботі розглядаються програмні та програмно-апаратні методи захисту для встановлення захищеної персональної інформаційної мережі житлового будинку. Аналізуючи проблеми звичайних абонентів, було виявлено, що більшість користувачів вибирають прості та ненадійні паролі для доступу, часто однакові для багатьох ресурсів.

Зважаючи на це, запропоновано впровадити авторизацію для входу в будь який Інтернет сервіс, портал чи сайт за допомогою дзвінка на телефон. Абоненту потрібно відповісти на дзвінок, щоб увійти до потрібної мережі.

Зміст ідеї стартапу та визначення її характеристик наведено в табл. 5.1 та табл. 5.2.

Таблиця 5.1 – Зміст ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Запропонувати аутентифікацію для входу в сервіси Інтернет за допомогую дзвінка .	1. Інформаційна безпека	Оптимізація захисту цінних ресурсів та інформації
	2. Персональне використання	Полегшення для входу на різні сайти; не потрібно запам’ятовувати довгі та різні паролі

Таблиця 5.2 – Визначення характеристик ідеї стартап-проекту

№ п/п	Техніко-економічні характеристики ідеї	(потенційні) товари/концепції конкурентів		W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
		Запропонований	Загальновживаний			

		метод	метод			
1.	Створення плагіну, що вносить в форму авторизації на Інтернет-ресурсі можливість входу за допомогою дзвінка.	Дає змогу	Дає змогу	Потребує детального опрацювання аспектів захисту	Підтримка користувача, оновлення ПО	Можливість зайняти актуальну у галузь у сфері інформаційного захисту
2.	Створення сервісу з установки і налаштування обладнання для авторизації за номером клієнтам(власникам сайтів)	Дає змогу	Дає змогу	Може потребувати достатніх кошт для створення	Цінова політика може не зацікавити потенційно клієнтів (власників сайтів)	Можливість комерційної та дотаційної реалізації

5.2 Технологічний аудит ідеї стартап-проекту

У наступній таблиці 5.3 наводиться оцінка можливостей технологічної реалізації ідеї стартапу, наведено технології, які можна застосувати для реалізації проекту.

Таблиця 5.3. Технологічна здійсненність ідеї проекту

№ п/п	Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
1	Створення плагіну для авторизації на різних Інтернет сайтах для авторизації	Програмне забезпечення та сервіс, що буде реалізовувати дзвінки (апаратне забезпечення - АТС)	Присутня	Доступна
2		Використання існуючих	Присутня	Доступна

	користувачів за допомогою дзвінка на телефон	апаратних систем стільникових мереж		
3		Розробка власних апаратно-програмних рішень	Відсутні на ринку в Україні	Доступна в випадку достатнього бюджету

Обрана технологія реалізації ідеї проекту: розробка сервісу для авторизації користувача за допомогою дзвінка на телефон за вказаним номером. Реалізується наступним чином:

У системі авторизації заявок три ланки- телефонний клієнт, АТС і БД-сервер, де зберігаються облікові записи користувачів. Процес:

1. Абонент вводить номер телефону, цим самим авторизується.
2. На сервері йде запит – певний логін намагається авторизуватися.
3. Коритсувач дзвонить за номером сервісу.
4. АТС визначає його номер і відхиляє дзвінок.
5. АТС передає в базу даних сервісу факт дзвінка.
6. База даних порівнює логін початкового запиту і номер, АТС висилає в додатку клієнта підтвердження або відмову в авторизації

5.3 Аналіз можливостей ринку для запуску проекту

У таблиці 5.4 показано попередню характеристику потенційного ринку стартап-проекту.

Таблиця 5.4. Попередня характеристика потенційного ринку стартапу

№ п/п	Показники ринку (найменування)	Характеристика
1	Кількість основних гравців, од	4
2	Обсяг продажів, грн/ум.од	180000
3	Тенденції ринку (якісна оцінка)	Зростає
4	Обмежень для входу (вказати характер обмежень)	Залучення потенційних клієнтів
5	Специфічні вимоги стандартизування та сертифікування	Ліцензія
6	Середня норма рентабельності в даній галузі, %	180000/95000 = 189%

У таблиці 5.5 показано характеристику потенційних клієнтів стартап-проекту

Таблиця 5.5. Характеристика потенційних клієнтів стартап-проекту

№ п/п	Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності поведінки потенційних цільових груп клієнтів	Вимоги споживачів до товару
1	Спрощення авторизації для соціальних мереж	Бізнес, Інтернет-користувачі	Необхідний рівень швидкості передавання даних для входу	Результат повинен відповідати найвищим стандартам якості
2	Авторизація в мобільних додатках для замовлення послуг	Бізнес, сфера послуг	Швидкість передавання даних для замовлень послуг	Результат повинен відповідати найвищим стандартам якості

У табл. 5.6 наведено основні загрози реалізації стартап-проекту.

Таблиця 5.6. Фактори загроз

№ п/п	Фактор	Опис загрози	Планове реагування компанії
1	Недостатній інтерес клієнтів	В випадку невдалого маркетингу клієнта можуть не зацікавити запропоновані послуги	Забезпечення додаткових сервісних послуг
2	Втрата конкурентних позицій	Втрата статусу надійного постачальника послуг	Якісний та кількісний приріст інтенсивності та виважена цінова політика

У табл.5.7 наведено основні можливості під час реалізації стартап-проекту.

Таблиця 5.7. Основні можливості

№ п/п	Фактор	Опис можливості	Планове реагування компанії
1	Лідерські позиції на ринку послуг інформаційної безпеки	Стрімке зростання попиту	Якісне та кількісне збільшення продукту, якісна підтримка користувача, постійні оновлення безпеки
2	Впровадження запропонованих технологій в уже існуючі системи соціальних мереж та мобільних додатків	Збільшення об’ємів закупівель	Якісне та кількісне збільшення обсягів продукту

Таблиця 5.8. Аналіз конкуренції

Особливості конкурентного середовища	Прояв даної характеристика	Вплив на діяльність підприємства (планові дії компанії для забезпечення конкурентоспроможності)
1.Конкуренція	Застосування вже існуючих технологій	Проведення стандартизації на високому рівні
2.Локальний	Відсутність єдиного постачальника послуг	Індивідуальний підхід до кожного

		клієнта та його апаратної частини
3.Міжгалузева	Відсутня	Відсутня
4.Товарно-видова	Використання стандартизованих технологій	Застосування загальновживаних апаратних засобів,за необхідності
5.Цінова	Використання високовартісних спеціалізованих комплексів	Можливість заощадити шляхом застосування загальновживаних апаратних засобів
6.Марочна	Кожна послуга повинна бути стандартизованою	Здобуття переваги на ринку інформаційних послуг

Таблиця 5.9 – Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари-замінники
	Апратні постачальники	Необхідність пошуку постачальників	Залучення малопопулярних постачальників	Незалежність у прийнятті клієнтських рішень	Надання переваги більш авторитетнимапаратним рішенням
Висновки:	Незначна	Можливість виходу на ринок є	Постачальники диктують цінову політику на	Клієнти диктують вимоги	Обмеження існують лише у

			обладнання	до якості	разі відмови від діагнос-тики

У табл. 5.10 наведено та обґрунтувано фактори конкурентноспроможності.

Таблиця 5.10. Обґрунтування факторів конкурентоспроможності

№ п/п	Фактор конкурентоспроможності	Обґрунтування (чинники, що роблять фактор порівняння конкурентних проектів значущим)
1	Раціональніша цінова політика	Можливість раціональнішого використання ресурсів
2	Забезпечення сервісних послуг	Сервісне обслуговування апаратної та програмної частини

У табл. 5.11 перелічено сильні та слабкі сторони проекту.

Таблиця 5.11. Порівняльний аналіз сильних та слабких сторін проекту

№ п/п	Фактор конкурентоспроможності	Бали 1-20	Порівняння рейтингу товарів-конкурентів						
			–3	–2	–1	0	+1	+2	+3
1	Раціональніша цінова політика	15	+						
2	Послуги сервісного обслуговування	12			+				
3	Періодична діагностика	7					+		
4	Потреба в залученні висококваліфікованих кадрів	7						+	

У табл.5.12 представлений SWOT-аналіз стартап-проекту.

Таблиця 5.12. SWOT- аналіз стартап-проекту

Сильні сторони: раціональна цінова політика, послуги сервісного обслуговування	Слабкі сторони: періодична діагностика, потреба в залученні висококваліфікованих кадрів
Можливості: Ексклюзивне використання нового методу, впровадження методу в існуючі мережеві логічні комплекси	Загрози: низька зацікавленість клієнтів, втрата конкурентспроможності

Альтернативи ринкового впровадження стартапу показані в табл.5.13.

Таблиця 5.13. Альтернативи ринкового впровадження проекту

№ п/п	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	Ймовірність залучення ресурсів	Терміни реалізації
1	Складання договорів з компаніями надавачами Інтернет послуг	висока	короткі
2	Застосування АТС для підвищення конкурентоспроможності та залучення нових спеціалістів для покращення програмної частини проекту	середня	середні

5.4 Розроблення ринкової стратегії проекту

Обгрунтування вибору цільових груп потенціійних споживачів показано в табл. 5.14.

Таблиця 5.14. Вибір цільових груп потенційних споживачів

№ п/п	Загальний профіль цільової групи потенційних клієнтів	Готовність сприйняття продукту споживачами	Орієнтовний попит цільової групи (сегменту)	Напруженість конкуренції в сегменті	Складність входу у сегмент

1	Власники мереж надання послуг та інформаційних ресурсів	Середня	Високий	Середня	Середня
2	Приватні мережі	Середня	Середній	Середня	Середня

Визначення базової стратегії розвитку наведено у табл. 5.15.

Таблиця 5.15. Визначення базової стратегії розвитку

№ п/п	Обрана альтернатива розвитку проекту	Стратегія охоплення ринку	Основні конкурентоспроможні позиції згідно з обраною альтернативою	Базова стратегія розвитку*
1	Застосування альтернативних технологій та пристроїв	Впровадження нового стандарту авторизації	Залучення ключових сервісів соціальних мереж	Стратегія диференціації
2	Бюджетність проекту	Оптимізовані ші затрати на обладнання, та послуги	Використання загальновживаних апаратних рішень замість спеціалізованих комплексів та нового обладнання	Стратегія лідерства по витратах

Визначення основної стратегії конкурентної поведінки показано в табл. 5.16.

Таблиця 5.16. Визначення базової стратегії конкурентної поведінки

№ п/п	Чи є проект унікальним на ринку?	Чи необхідно буде компанії шукати нових споживачів, чи опрацьовувати існуючих у конкурентів?	Чи необхідно компанії копіювати основні характеристики товару конкурента?	Стратегія конкурентної поведінки*
1	Ні	Опрацьовувати існуючих та шукати нових	Так	Стратегія виклику лідера

Визначення стратегії позиціонування показано в табл. 5.17.

Таблиця 5.17. Визначення стратегії позиціонування

№ п/п	Вимоги цільової аудиторії до товару	Основна стратегія розвитку	Основні конкурентоспроможні позиції стартап-проекту	Визначення асоціацій, які сформують комплексну позицію стартап-проекту (три основних)
1	Належна висока якість послуг	Стратегія диференціації	Оптимізація, гарант якості, спрощення дій для авторизації	Якість, підтримка, надійність
2	Невисокі витрати	Стратегія лідерства по витратах	Універсальність запропонованого рішення	Універсальність, економічна доцільність

5.5 Розроблення маркетингової програми стартап-проекту

Основні переваги концепції потенційного товару показано в табл. 5.18.

Таблиця 5.18. Визначення основних переваг концепції потенційного товару

№ п/п	Потреба	Вигода, яку пропонує товар	Основні переваги перед конкурентами (існуючі або потенційні)
1	Якість	Висока якість і простота у використанні, надійність	Постійна підтримка користувача, оффлайн підтримка.
2	Невисока вартість	Оптимальне використання коштів, не потрібно купувати нове обладнання	Невисока вартість

Виявлено три рівні моделі товару. Зміст та складові рівнів товару показано в табл. 5.19.

Таблиця 5.19. Опис трьох рівнів моделі товару

Рівні товару	Зміст та складові

I. Товар за задумом	Якісний товар та послуги, стандартизована якість послуг та обладнання		
II. Товар у реальному виконанні	Властивості/характеристики	М/Нм	Вр/Тх /Тл/Е/Ор
	1)Вартість обслуговування, 2)Кількість комплектів програми 3)Строк безвідмовної експлуатації 4)Технологічна собівартість товару	1) М 2) М 3) М 4) М	1)Е 2) Пр 3)Нд 4)Тх
	Якість: дослідження досвіду конкурентів, постійне обслуговування та підтримка програмного обладнання		
	Доставка, встановлення і налаштування		
	Марка: інформаційна безпека мережі		
III. Товар із підкріпленням	До продажу – програмне забезпечення та апаратний комплекс		
	Після продажу – обслуговування та сервісна підтримка		

Визначення цінової політики на послугу показано в табл. 5.20.

Таблиця 5.20. Визначення меж встановлення ціни

№ п/п	Цінова політика товарів-замінників	Цінова політика на товари-аналоги	Рівень купівельної спроможності цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу
1	5000у.о./од. (стандартна методика)	-	Високий	Н.300 у.о. – В.1000 у.о. (Товар) Н.100у.о. – В.400у.о. (Послуга)

Створення системи збуту послуги вказано у табл. 5.21.

Таблиця 5.21. Створення системи збуту

№ п/п	Закупівельна поведінка цільових клієнтів	Функції збуту, що повинен забезпечувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
1	Орієнтована на максимальний дохід від існуючого обладнання та вкладених коштів	Поставки якісного, точного та надійного товару	Значна	Договірна система збуту

Концепції маркетингових комунікацій показано в табл. 5.22.

Таблиця 5.22. Концепція маркетингових комунікацій

№ п/п	Специфіка поведінки цільових клієнтів	Канали комунікацій цільових клієнтів	Основні методи позиціонування	Завдання рекламного звернення	Концепція рекламного звернення
1	Зацікавленість в точному та якісному продукті з раціональним використанням ресурсів	Мережні ресурси	Гарантія якості та стандартизація, сервісна політика	Привернути увагу до покращень, пов’язаних із зростаючою популярністю послуг	Позиціонування центру синхронізації відправною точкою на шляху до над якісного контенту
2	Зацікавленість у великих об’ємах продукції із дотриманням умов якості	Мережні ресурси	Глибина каналу постачальників, гарант якості	Привернути увагу до переваг первісності та в глибині каналу постачання	Позиціонування послуг центру синхронізації єдиним раціональним шляхом забезпечення стабільного трафіку

Висновки до 5 розділу.

Встановлено, що комерціалізацію стартап-проекту щодо застосування та розвитку запропонованого програмного рішення авторизації абонентів в

мережах Інтернет та сервісів з надання послуг вважати доцільною. На ринку інформаційних у світі існує суттєвий попит на дану пропозицію, який зараз задовольняють програми-замінники та більш дорогі рішення. В Україні прямих конкурентів немає, оскільки технології для впровадження та продажу цього продукту лише вийшли на ринок. Рентабельність на ринку послуг забезпечить в першу чергу можливість впровадження нових способів захисту та збереженню паролів на основі існуючої апаратної частини, й як наслідок економічну доцільність та універсальність.

Можливість виходу на ринок є високою, оскільки в Україні немає схожих сервісів та продукт стартапу пропонує інше рішення для аутентифікації абонентів – коли клієнт, власник сервісу послуг, власне сам є власником баз даних своїх клієнтів. Конкуренті спроможності проекту реалізовано внаслідок можливості зайняти порожню нішу в Україні та надати гарний рівень підтримки продукту. Це є перевагою і основним критерієм входження на ринок запропонованого рішення.

3. Обрана альтернатива впровадження – пошук альтернативних технологій та пристроїв для авторизації абонентів у мережі. Позитивні умови для просування проекту зумовлені вимогами ринку, а саме прагнення зростання у сфері послуг (кур’єрські доставки, таксі) у зв’язку з карантином.

ВИСНОВКИ

В даний час власники та адміністратори мережі займаються захистом своїх ресурсів, надаючи пріоритет розгортанню заходів безпеки перед наданням будь-яких мережевих послуг. Щоб створити безпечну мережеву систему, адміністратору мережі слід вибрати правильний тип технології, яка відповідає цілям компанії та вимогам безпеки. Метою цього проекту було вивчення дослідження сучасних методів захисту для домашньої інформаційної мережі житлового будинку.

Атака на комп'ютерну систему може статися в будь-який час з будь-якого місця, і тому захист комп'ютера та мережевої системи залишається без вибору. Захист мережі житлового будинку вимагає розробки плану та політики безпеки, які визначають, що потрібно захищати і від кого, а потім застосовувати правильні заходи безпеки, щоб зупинити атаки та взламування. Систему потрібно постійно контролювати на предмет загрози та атак, що надходять зсередини та зовні мережевої системи.

Це дослідження виявило, що жодна мережева система не захищена від нападу, і виявило джерело вразливостей системи, а також конфігурація та слабкість технологій. Тому було запропоновано цілу низку рішень для захисту на кожному рівні, включаючи апаратні та програмно-апаратні заходи безпеки.

Проводячи дослідження методів захисту, не можна надати перевагу конкретному. Ефективність заходів є найвищою коли використовуються різні на усіх площинах. Далі наводиться досліджений комплексний підхід до захисту мережі зважаючи на потреби абонентів:

1. Firewall – міжмережевий екран, на вході в мережу для управління доступом до публічної мережі серверів, вхідними та вихідними пакетами даних, запропоновано Cisco (ASA 5505)
2. Технологія IDS – на вході мережі після Firewall набуває вищої ефективності, адже вона контролює уже відсортований трафік мережевим фільтром для зниження навантаження мережі. Технологія налаштована утилітою Snort;
3. Сканування рівня кожного вузла - пропонується сканер рівня вузла Assuria Auditor . Тобто забезпечується захит не тільки на рівні мережі, а й на рівні вузла.
4. Встановлення антивірусних програм на кожному абонентському комп'ютері та серверах. Даний програмний захист допомагає користувачам

мережі контролювати свою захищеність від зловмисників та шкідливих програм. Пропонується Microsoft Security Essentials - безкоштовний антивірус, дає можливість налаштовувати параметри сканування, забезпечує безперервний захист в реальному часі.

5. Захист мережі Wi-Fi абонентів: вибір типу безпеки мережі WPA/WPA2, встановлення надійного WPA, та обов'язкова заміна паролю адміністратора на доступ до конфігурації пристрою.

6. Фізичний захист: встановлення мережевого обладнання в надійному відповідному місці.

Усі перераховані методи не є стовідсотковою гарантією захисту, адже технології з плином часу активно змінюються і прогрес росте. Тому ще один важливий аспект – методи захисту мають відповідати часу і технологіям, постійно оновлюватись, адміністратори мережі повинні шукати нові рішення і технології.

ПЕРЕЛІК ПОСИЛАНЬ

1. ITU-T, “Overview of the Internet of Things,” Recommendation Y.2060, June 2012.
2. Cisco Systems, “The Internet of Things Reference Model,” White Paper, 2014. http://www.iotwf.com/
3. Gen, H.P.-C.S.A. Controllers, R.: Hewlett-Packard Enterprise Development LP. Citeseer (2015)
4. Dr. G. F. Ali Ahammed, Dr. Reshma Banu, Nasreen Fathima, «An Approach to Secure Communication in IoT (Internet of Things)», Conference Paper · February 2016
5. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / под. редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012.
6. Ли П. Архитектура интернета вещей / пер. с анг. М. А. Райтмана. – М.: ДМК Пресс, 2019. – 454 с.: ил.
7. В.Д. Мунистер. Дом который построил сам себя: Учебно-практическое издание – 2020.
8. Бондарев В.В. Анализ защищенности и моніторинг компьютерных сетей. Методы и средства: учебное пособие / В.В. Бондарев – Москва: Издательство МГТУ им. Н. Э. Баумана, 2017.
9. Rita Dewanjee, Mr. Pushpak Verma. Cryptography Techniques and Internet of Things. MSIT, MATS University, 2018
10. Priscilla Oppenheimer. Top-Down Network Design. Indianapolis, USA: Cisco Press; 2011.
11. Etutorials. Flat Network Topology [online]. USA: etutorials; January 2013.
12. URL: http://etutorials.org/Networking/lan+switching/Chapter+10.+LAN+Switched+Network+Design/Flat+Network+Topology/. Access Доступ 18 вересня, 2020 р.
13. Dan Dinicolo. Understanding Network Models/The Cisco Network Design Model [online]. Canada: WebProNews; 2013.
14. URL:http://www.webpronews.com/understanding-network-models-the-cisconetwork-design-model-2004-02. Доступ 18 вересня, 2020 р.
15. Cisco. Network Topology and LAN Design [online]. USA: Cisco press; January 14, 2000.

16. URL:http://networkworld.com/ns/books/ciscopress/samples/0735700745.pdf. Доступ 18 вересня, 2020 р.
17. Randy Ivener. CCNP1:Advance Routing. Indianapolis, USA: Cisco Press; 2004.
18. Paul Boger. CCNA Exploration LAN Switching and Wireless version 4.0. Indianapolis, USA: Cisco Press; 2010.
19. Sean Wilkins, Franklin H.Smith III. CCNP Security SECURE 642-637 Offical Cert
20. Guide. Indianapolis, USA: Cisco Press; 2010.
21. John E. Canavan. Fundamentals of Network Security. London, Britain: Artech House; 2001.
22. R. Shirey, editor. Internet Security Glossary [online]. USA: IETF; 2000.
23. Gregory B. White, Eric A.Fisch, UWdo w. Pooch. Computer System and Network Security. USA: CRC press; 2000.
24. Randy Marchany. Computer and network security in Higer Educstion. USA:Jossey-Bass Inc.; 2003.
25. Steve Elky. An Introduction to Information System Risk Management. USA: SANS Institute; May 31, 2006.
26. Joe Harris. Cisco Network Security Little Balack Book. Arizona, USA: The Coriolis Group, LLC; 2002.
27. B. Fraser, editor. Site Security Handbook. USA: IETF; 1997.
28. URL: https://wiki.merionet.ru/seti/31/ustanovka-i-nastrojka-utility-dlja-obnaruzhenija-vtorzhenij-v-seti-snort/
29. Александров Г.Д. Проектирование защищенной корпоративной сети передачи данных, Российская неделя высоких технологий, выпуск от 24.04.18
30. URL: https://creately.com/blog/examples/network-diagram-templates-creately/
31. URL: https://hd01.ru/info/kak-zashhitit-lokalnuju-set/
32. URL:https://silo.tips/download/assuria-auditor-the-configuration-assurance-vulnerability-assessment-change-dete
33. URL: https://xakep.ru/2012/10/29/ids-ips/#toc10.

ДОДАТОК А

Abstract

In the modern world, network and information technologies are actively developing. Currently, it is impossible to find a functional enterprise that operates without the possibility of the Internet and a proper connection to the data network. Such a network will try and optimize a large number of tasks, such as information exchange, work on documents, membership in programs, exchange of resources and information about them.

People have been protecting their property since ancient times. Lack of protection can lead to the loss of property of human life. Over time, the problem of protection of information and digital property has become relevant. In this way, computer resources must be protected from internal and external attackers.

Information is a very valuable resource, so attackers often try to access both corporate and home networks. The main reason for the introduction of network security is the protection of networks and system resources connected to the network. Information is in any case determined by the valuable power of the network, and it loses access to it, which can generate money or otherwise cause a catastrophe. Hacking can lead to a variety of consequences: viewing data, earning malware, and reducing all data. Then you should pay attention to the protection of networks, look for developed and identified possible threats that may invite the school to the current system and resources. That is why it is extremely important today for companies to pay special attention to raising the level of their security levels.

The introduction of security controls in a network environment allows the network system to work accordingly. The main reason for the introduction of network security is the protection of networks and system resources connected to the network.

Network owners and administrators are currently protecting their resources, prioritizing the deployment of security measures over the provision of any network services. To create a secure network system, the network administrator must select the correct type of technology that meets the company's goals and security requirements. The purpose of this project was to study the study of modern protection methods for home information network of a residential building.

An attack on a computer system can occur at any time from anywhere, so there is no choice but to protect your computer and network system. Protecting a residential network requires a security plan and policy that defines what needs to be protected and from whom, and then takes the right security measures to stop attacks and hacking. The system must be constantly monitored for threats and attacks coming from inside and outside the network system.

This study found that no network system is vulnerable to attack, and identified the source of the system's vulnerabilities, as well as the configuration and weakness of the technology. Therefore, a number of security solutions have been proposed at each level, including hardware and software-hardware security measures.

When researching methods of protection, you can not give preference to specific. The effectiveness of measures is highest when different ones are used on all planes. The following is a comprehensive approach to network protection taking into account the needs of subscribers:

1. Firewall - a firewall, at the entrance to the network to control access to the public network of servers, incoming and outgoing data packets, proposed by Cisco (ASA 5505)

2. IDS technology - at the network input after the Firewall becomes more efficient, because it controls the already sorted traffic by the network filter to reduce network load. The technology is configured with the Snort utility;

3. Scan level of each node - Assuria Auditor node level scanner is offered. That is, protection is provided not only at the network level, but also at the node level.

4. Installation of anti-virus programs on each subscriber's computer and servers. This software protection helps network users to control their protection against malware and malware. Microsoft Security Essentials is offered - a free antivirus, allows you to configure scan settings, provides continuous real-time protection.

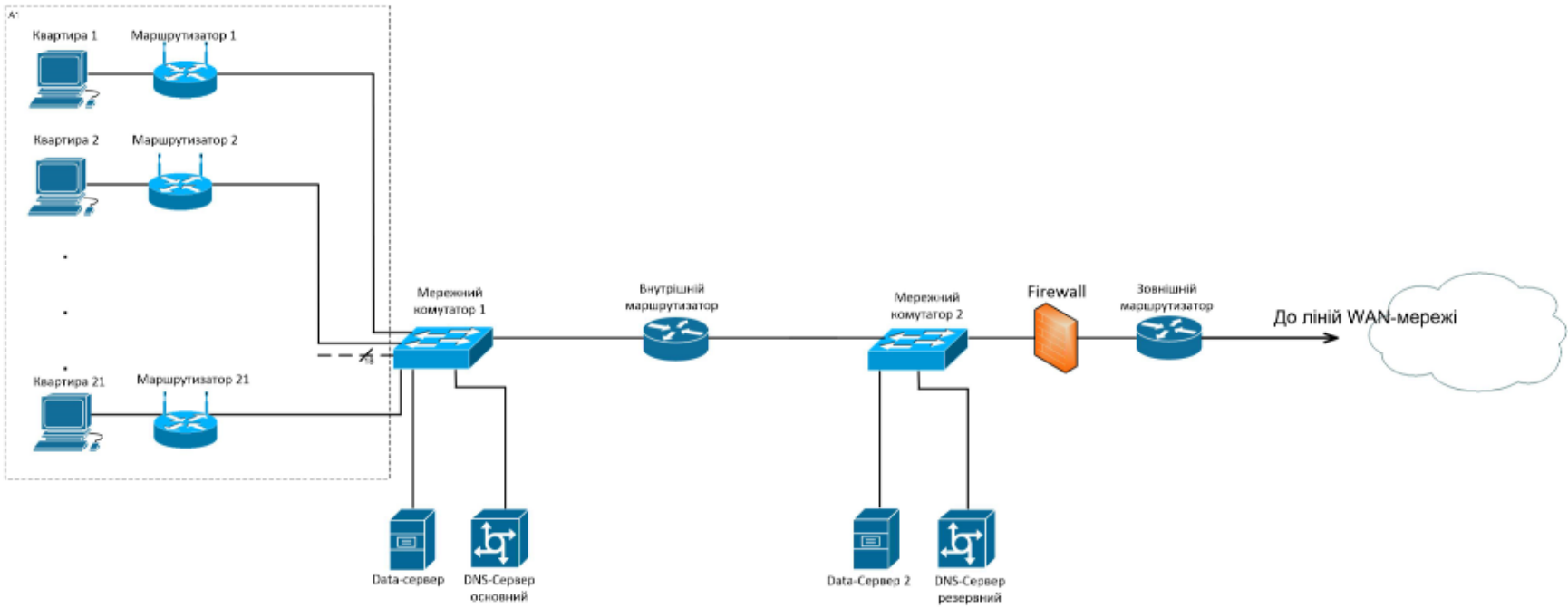
5. Wi-Fi network security: choose the type of security of the WPA / WPA2 network, install a reliable WPA, and change the administrator password to access the device configuration.

6. Physical protection: installation of network equipment in a reliable appropriate place.

All these methods are not a 100% guarantee of protection, because technologies are actively changing over time and progress is growing. Therefore, another important aspect - security methods must be up to date and technology, constantly updated, network administrators must seek new solutions and technologies.

ДОДАТОК Б

Графічне зображення персональної інформаційної мережі житлового будинку


Квартира 1
Маршрутизатор 1
Квартира 2
Маршрутизатор 2
Квартира 21
Маршрутизатор 21
Мережний комутатор 1
Внутрішній маршрутизатор
Мережний комутатор 2
Firewall
Зовнішній маршрутизатор
До ліній WAN-мережі
Data-сервер
DNS-Сервер основний
Data-Сервер 2
DNS-Сервер резервний