

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ**

Пояснювальна записка

до бакалаврської роботи
на тему:

**«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО
ПОБУДОВИ ЗАХИЩЕНОЇ СИСТЕМИ « РОЗУМНИЙ» БУДИНОК З
ВИКОРИСТАННЯМ ОБЛАДНАННЯ CISCO»**

Виконав студент 4 курсу, групи БСД-42
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна
та кібернетична безпека»

(шифр і назва спеціальності)

Чорній О.С.

(прізвище та ініціали)

Керівник Довженко Н.М.

(прізвище та ініціали)

Рецензент _____

(прізвище та ініціали)

Нормоконтролер _____

(прізвище та ініціали)

КИЇВ – 2023

ВСТУП

Актуальність дослідження. «Розумні» будинки - це технологія, яка дозволяє людям контролювати та оптимізувати використання ресурсів та різних систем у будинку. Ця інноваційна технологія стає все більш популярною та доступною для широкого загалу. Історія розвитку «розумних» будинків, їх принцип роботи, основні складові та технології, що використовуються для їх реалізації. Окремо будуть розглянуті переваги та недоліки використання розумних будинків, а також перспективи їх розвитку та інтеграції в різні сфери життя. Зараз «розумні» будинки можуть бути управляні з допомогою мобільних додатків, голосових помічників, а також встановленням різноманітних датчиків та інших сенсорів, які дозволяють автоматично регулювати системи опалення, кондиціонування, освітлення та інші системи.

Крім того, використання обладнання Cisco для створення «розумного» будинку дозволяє забезпечити стійкий та безпечний зв'язок між різними пристроями, що забезпечує високу надійність та швидкість обміну даними. Також, використання технологій Cisco дозволяє забезпечити захист від вторгнень та зламів, що є надзвичайно важливим у світі, де кібербезпека стає все більш актуальною темою.

Об'єкт дослідження – система «розумний» будинок.

Предмет дослідження – методи та засоби управління та об'єднання автоматизованих систем «розумного» будинку з використанням обладнання Cisco.

Мета роботи – розробка рекомендацій щодо захисту «розумних» будинків на базі обладнання Cisco.

Завдання бакалаврської роботи:

- дослідити теоретичні аспекти технології «розумний» будинок та існуючих рішень на ринку.
- проаналізувати технічні можливості та функціонал обладнання Cisco для створення «розумного» будинку.

- дослідити архітектуру мережі та інфраструктури для підключення обладнання Cisco.
- розробка рекомендацій щодо вдосконалення та розвитку системи «розумного» будинку на базі обладнання Cisco.

Методи дослідження – опрацювання технічної літератури за даною темою, аналіз експлуатаційної документації інструментів, проведення тестування інструментів, порівняльний аналіз сервісів

Практичне значення одержаних результатів: рекомендації щодо використання розробленої системи керування «розумним» будинком на базі обладнання Cisco в реальних умовах.

1 АНАЛІЗ ОСОБЛИВОСТЕЙ ТЕХНОЛІГІЙ «РОЗУМНИЙ» БУДИНОК

1.1 Поняття « Розумний» дім

«Розумний» дім (Smart Home) - це дім, обладнаний спеціальною технологією, що дозволяє автоматизувати різноманітні процеси в будинку. Він використовує високотехнологічні пристрої та системи, які забезпечують комфорт, безпеку, економію енергії та забезпечення життєвого простору.

«Розумний» дім може включати в себе такі елементи, як автоматизація опалення, кондиціонування повітря, освітлення, звукові системи, електронні системи безпеки, домашні кінотеатри, інтернет речей та інші елементи, що забезпечують підвищення комфорту життя в будинку.

Одним з ключових переваг «розумного дому» є можливість керування всіма пристроями та системами віддалено з використанням смартфонів, планшетів або комп'ютерів. Це дозволяє власнику будинку контролювати температуру, освітлення, безпеку та інші аспекти життя в будинку, не знаходячись у ньому.

Окрім цього, розумний дім дозволяє заощаджувати енергію та знижувати рівень викидів в атмосферу. Система може регулювати температуру та освітлення в будинку в залежності від наявності людини в кімнаті, часу доби, погодних умов тощо.

Нарешті, «розумний» дім є зручним інструментом для забезпечення безпеки в будинку. Системи безпеки можуть бути підключені до сигналізації, камер відеоспостереження та інших пристроїв, що дозволяє моніторити діяльність в будинку та реагувати на небезпеку в реальному часі.

Він є продуктивною інвестицією в майбутнє, особливо для тих, хто планує будувати новий будинок або робити капітальний ремонт вже існуючого приміщення. Він може забезпечити не тільки комфорт і безпеку, але й значну економію коштів на різних аспектах домашнього життя.

Варто зазначити, що «розумний» дім може бути вартістю достатньо великою, в залежності від технологій та систем, які будуть встановлені. Крім того, інтеграція різних пристроїв та систем може бути складною задачею, яка потребує високого рівня експертизи та професійного підходу.

Таким чином - це інноваційний підхід до життя, який забезпечує власнику будинку більшість необхідних елементів для комфортного та безпечного життя. Він дозволяє зробити дім більш ефективним, енергоефективним та функціональним, що допомагає знизити рівень витрат та підвищити якість життя.

«Розумні» будинки - це не нове поняття і їх історія розвитку налічує кілька десятиліть. Перші елементи автоматизації в будинках почали з'являтися у 1970-х роках, коли розумний дім був названий «комп'ютерним будинком». Тоді комп'ютери та пристрої, які контролюють різні системи в будинку, були рідкістю, а ціна на них була дуже високою. Ці системи зазвичай використовувалися для керування опаленням, кондиціонуванням повітря, освітленням та системами безпеки.

У 1980-х роках із зростанням популярності персональних комп'ютерів з'явилася можливість використовувати їх у «розумних» будинках. Власники будинків змогли здійснювати керування своїми системами з будь-якого місця в будинку або за його межами.

У 1990-х роках з'явилися нові технології, такі як інтернет, бездротові технології та Bluetooth, які дозволили власникам будинків керувати своїми системами віддалено з будь-якої точки світу. Більшість розумних систем були незалежними одна від одної, і не можна було забезпечити повної інтеграції.

У 2000-х роках з'явилася можливість інтегрувати різні системи в одну цілісну систему керування. Власники «розумних» будинків могли керувати всіма системами з одного інтерфейсу, що значно спрощувало процес керування. В цей час відбулося значне зростання ринку «розумних» будинків, і на ринку з'явилося багато нових компаній, які пропонували рішення для автоматизації будинків.

Сьогодні «розумний» будинок - це досить популярне рішення, яке забезпечує зручність, комфорт та енергоефективність. Власники можуть керувати різними

системами в будинку, такими як опалення, кондиціонування повітря, освітлення, звукова та відео системи, безпека, терморегулювання та інші. Це дозволяє знижувати витрати на енергоспоживання та зберігати енергію, підвищувати рівень комфорту та безпеки, та знижувати кількість рутинних задач.

Сучасні рішення для «розумних» будинків включають в себе використання датчиків, мікроконтролерів, мережевих технологій та інтернету речей. Компанії, такі як Apple, Google та Amazon, також пропонують свої рішення для «розумних» будинків, такі як голосові помічники, які дозволяють керувати різними системами в будинку за допомогою голосу.

Майбутнє «розумних» будинків виглядає досить захоплюючим. З'являються нові технології, які дозволяють підвищувати рівень автоматизації та безпеки в будинку. Наприклад, системи штучного інтелекту можуть навчитися аналізувати дані про поведінку власників будинку, що дозволить забезпечити більш ефективне керування системами.

Також з'являються нові технології, які дозволяють виробникам енергії, наприклад, сонячних панелей, забезпечувати енергію для будинків, що значно знижує витрати на енергоспоживання та допомагає зменшувати вплив на довкілля.

У загальному, розумні будинки є важливим тим, що забезпечують ряд переваг, включаючи більшу зручність та комфорт, підвищення безпеки, підвищення енергоефективності та зменшення негативного впливу на довкілля. «Розумні» будинки також стають більш доступними для власників будинків, завдяки зниженню вартості технологій та збільшенню їхньої доступності.

Одним з найбільш яскравих прикладів «розумних» будинків є "Смарт-Хаус" від компанії X10. У 1975 році компанія X10 створила систему, яка дозволяла керувати електроприладами за допомогою сигналів, які передавалися через електричну мережу будинку. Система X10 мала можливість керувати світлом, кондиціонерами, опаленням та іншими пристроями. Система відразу здобула популярність, але зазнавала критики через надмірний рівень шуму в мережі електроживлення.

З розвитком технологій, з'явилися більш ефективні та прогресивні системи, які забезпечують більшу зручність та ефективність використання. Наприклад, компанія Nest створила "розумний» термостат, який автоматично регулює температуру в будинку в залежності від присутності людей, пори року та інших факторів. Також, на ринку з'явилися рішення від компаній Apple, Google та Amazon, які дозволяють керувати різними системами в будинку за допомогою голосу та інших простих команд.

У майбутньому «розумні» будинки можуть стати стандартом життя, оскільки технології стають більш доступними та простими у використанні, а також через їхню енергоефективність та спроможність знижувати витрати на електроенергію. Вже зараз можна побачити збільшення кількості пристроїв у «розумних» будинках, таких як датчики температури та вологості, камери відеоспостереження, розумні витратоміри, дверні замки, системи контролю доступу та інші.

Однак, багато з цих ризиків можна уникнути або пом'якшити за допомогою застосування відповідних технологій та заходів безпеки, таких як захист мережі від хакерських атак, використання надійних паролів та багатофакторної аутентифікації, системи контролю доступу до різних ділянок будинку та інші.

Загалом, «розумний» будинок - це інноваційний підхід до житлового будівництва, який має великий потенціал у забезпеченні зручності, безпеки та енергоефективності. При цьому важливо пам'ятати про необхідність застосування відповідних технологій та заходів безпеки, щоб уникнути неприємностей та забезпечити безпеку та комфорт жителів будинку.

Одним з основних напрямків розвитку «розумних» будинків є інтеграція різних систем керування та автоматизації в єдину платформу. Це дозволяє забезпечити більш ефективне та зручне керування всіма системами будинку, а також збільшує можливості для їх взаємодії та оптимізації.

Наприклад, системи розумного освітлення можуть залежати від зовнішньої освітленості, температури повітря та руху в будинку. Вони можуть автоматично вимикатись, коли нікого немає в кімнаті, або залежно від пори дня вмикатись і вимикатись автоматично. Системи "розумного» опалення можуть контролювати

температуру в кожній кімнаті, а також враховувати рівень вологості і забезпечувати автоматичний контроль за вікнами та дверима, щоб зберегти енергію.

Додатково, «розумні» будинки можуть бути підключені до інших розумних пристроїв, таких як розумні телевізори, розумні холодильники та інші, що дозволяє жителям більш ефективно керувати своїм життям та додатково зменшувати витрати енергії та інших ресурсів.

Розвиток «розумних» будинків продовжується, а їх можливості та функціонал лише зростають. Розумні будинки дозволяють забезпечувати вищий рівень комфорту, безпеки та енергоефективності, що є особливо важливим у сучасному світі. Для подальшого розвитку ринку розумних будинків важливо постійно вдосконалювати технології та забезпечувати надійну та безперервну роботу систем. Крім того, важливо забезпечити доступність технологій «розумних» будинків для широкого кола людей.

Ще одним з напрямків розвитку «розумних» будинків є використання штучного інтелекту та машинного навчання. Це дозволить системам «розумного» будинку стати більш адаптивними до поведінки та потреб жителів, а також забезпечує більш точне прогнозування та оптимізацію роботи систем будинку. Наприклад, система «розумного» будинку може самостійно навчитись, коли відкривати вікна для провітрювання, коли включати опалення, а коли - вимикати його. Це дозволить забезпечити економію енергії та зробити життя в розумному будинку ще більш комфортним та зручним [1].

У майбутньому можна очікувати ще більшого поширення «розумних» будинків та їх інтеграції в інші сфери життя, такі як офіси, громадські будівлі та міста. Застосування розумних технологій може значно полегшити життя людей, збільшити ефективність використання ресурсів та зменшити вплив людства на довкілля.

Отже, «розумні» будинки - це не просто мода чи нова технологія, а спосіб поліпшення якості життя та збереження ресурсів. З кожним роком ця технологія стає все більш доступною та розвиненою, що дозволяє її застосування в різних галузях. Важливо продовжувати розвивати цю технологію та забезпечувати

безперебійну роботу систем «розумних» будинків для їх ефективного використання та популяризації серед населення.

1.2 Історія розвитку «розумних» будинків

Історія розвитку «розумних» будинків почалася в 1975 році, коли компанія X10 створила перший прототип системи дистанційного керування побутовими пристроями. Ця технологія дозволяла керувати електроприладами з використанням комп'ютера та радіохвиль.

Протягом наступних років, технології «розумних будинків» стали все більш складними та розширеними, з'явилися нові можливості керування освітленням, опаленням, кондиціонуванням повітря, безпекою та іншими системами.

Siemens та Legrand випустили перші системи керування освітленням, які дозволяли вмикати та вимикати лампи в різних частинах будинку за допомогою одного інтерфейсу. В цей період часу з'явилися інші компанії, такі як Crestron, AMX та Savant, які пропонували інтегровані рішення для управління будинками.

У 2000-х роках технології «розумних» будинків стали ще більш складними та розширеними, з'явилися нові можливості керування з допомогою мобільних додатків, голосових помічників та інших інтерфейсів. З'явилася можливість інтегрувати системи управління освітленням, опаленням, кондиціонуванням повітря та іншими системами з системами безпеки, розваг та енергозбереження.

Сьогодні «розумні» будинки можуть включати в себе велику кількість різноманітних сенсорів та пристроїв, які забезпечують комфорт, безпеку та енергоефективність. Інтеграція систем управління дозволяє власникам будинку контролювати роботу будь-якої системи з одного мобільного інтерфейсу, незалежно від того, де вони знаходяться.

Зараз «розумні» будинки можуть виконувати безліч функцій. Вони можуть контролювати температуру та вологість, регулювати освітлення в залежності від часу доби, присутності людей або стану погоди, запускати пилососи, регулювати

звук та музику у будинку, відкривати двері та вікна, контролювати систему безпеки та багато іншого.

Також на сьогоднішній день відбувається інтенсивний розвиток технологій Інтернету речей (IoT) та штучного інтелекту, які дозволяють «розумним» будинкам бути ще більш ефективними та корисними для користувачів. Тепер «розумні» будинки можуть навіть навчатися від своїх власників та адаптуватися до їхніх потреб, збираючи та аналізуючи дані про звички та вимоги користувачів.

У сьогоднішній час «розумний» будинок є символом майбутнього, де технології стають ще більш інтегрованими та ефективними. Він дозволяє власникам будинку контролювати свій дім за допомогою різних інтерфейсів, що забезпечує зручність, комфорт та безпеку. «Розумні» будинки можуть забезпечувати економію енергоресурсів та зниження витрат на опалення, освітлення та інші системи, що є важливим аспектом у сучасному світі, коли енергетичні ресурси дедалі більше дорожчають.

Однак, разом із зростанням популярності «розумних» будинків, постають і питання щодо приватності та безпеки даних користувачів. Збір та обробка персональних даних можуть бути використані зловмисниками для злочинних дій, тому необхідно забезпечити надійну систему захисту від несанкціонованого доступу до даних.

Також існує проблема стандартизації технологій та інтерфейсів для розумних будинків. Існують різні стандарти та протоколи, що використовуються в різних системах, що ускладнює інтеграцію різних компонентів між собою.

Загалом, можна сказати, що «розумні» будинки - це технологія, яка не зупиниться на досягнутому і буде продовжувати розвиватися та вдосконалюватися. Вона дозволяє зробити життя людей більш комфортним та зручним, допомагає зберігати енергоресурси та забезпечувати безпеку власників будинків. Зростання популярності розумних будинків, сьогодні, є свідченням того, що технології стають ще більш інтегрованими та доступними для людей, і ми можемо очікувати далій розвиток цієї галузі у майбутньому.

Однією з найбільш важливих переваг «розумних» будинків є їх можливість зберігати енергію та знижувати витрати на комунальні послуги. Завдяки автоматизації опалення, кондиціонування повітря та освітлення, можна знизити витрати на електроенергію та газ на 20-30%. У деяких випадках, ця економія може досягати 50%.

«Розумні» будинки можуть допомогти власникам знизити витрати на страхування, оскільки вони забезпечують підвищену безпеку будівель та майна. Системи відеоспостереження та датчики пожежі можуть запобігти злочинам та знизити ризик виникнення небезпечних ситуацій.

«Розумні» будинки забезпечують більш високий рівень комфорту та зручності. Інтерфейси управління дозволяють власникам легко контролювати всі системи та пристрої в будинку, віддалено керувати освітленням, опаленням та кондиціонуванням повітря. Крім того, розумні системи можуть допомагати людям із фізичними обмеженнями, забезпечуючи їм більш незалежний та комфортний спосіб життя.

Разом із зростанням популярності постають і питання щодо приватності та безпеки даних користувачів. Збір та обробка персональних даних можуть бути використані зловмисниками для злочинних дій, тому необхідно забезпечити надійну систему захисту від несанкціонованого доступу до даних.

Існує проблема стандартизації технологій та інтерфейсів об'єднання різних систем управління в одну єдину платформу. Це може створити труднощі для власників будинків, які хочуть використовувати продукти різних виробників.

Іншою проблемою є вартість встановлення та безпосередньо обслуговування «розумного» будинку. Системи управління можуть бути дорогими, і їх встановлення вимагає кваліфікованих фахівців. Крім того, «розумний» будинок потребує постійного обслуговування та оновлення програмного забезпечення, що може збільшувати витрати на його експлуатацію.

Незважаючи на ці проблеми, «розумні» будинки все більше стають популярними серед власників нерухомості. За прогнозами аналітиків, ринок розумних будинків зростатиме і в 2022 році досягне 174 мільярдів доларів. Це

свідчить про те, що «розумні» будинки є майбутнім технології для покращення якості життя людей [2].

Загалом, історія розвитку «розумних» будинків почалася більше 100 років тому, коли люди стали розвивати системи автоматизації для покращення комфорту та енергоефективності будівель. З часом, з'явилися нові технології та пристрої, що дозволили створити сучасні «розумні» будинки, які можуть автоматично керувати всіма системами в будинку, забезпечуючи максимальний комфорт та ефективність, та зменшуючи витрати на енергію та комунальні послуги.

1.3 Основні характеристики «розумного» будинку

Основна ідея «розумного» дому полягає в тому, щоб об'єднати різні системи управління будинком в одну інтегровану платформу, яка може керувати різними пристроями та пристроїми, що забезпечують комфорт, безпеку, енергоефективність та розваги в будинку.

Основні характеристики розумного дому включають:

1) Автоматизація: «Розумний» дім повинен мати здатність автоматично керувати різними пристроями та системами в будинку без участі людини. Наприклад, автоматичне керування освітленням, терморегулюванням, затворами на вікнах та дверях.

2) Інтеграція: «Розумний» дім повинен бути здатний інтегрувати різні системи в будинку, такі як системи освітлення, опалення, вентиляції, безпеки, розваг та інших, в одну платформу для зручного керування.

3) Керування здалеку: «Розумний» дім повинен бути здатний керуватися здалеку через мобільний додаток або веб-інтерфейс. Це дає можливість власникам будинку керувати різними пристроями та системами, навіть якщо вони знаходяться далеко від будинку.

4) Безпека: «Розумний» дім повинен бути оснащений системами безпеки, такими як системи відеоспостереження, датчики диму та вуглекислого газу,

датчики протікання води, що дозволяють вчасно виявити небезпечні ситуації та запобігти їм.

5) Енергоефективність: «Розумний» дім повинен бути здатний ефективно використовувати енергію, зменшуючи витрати на енергоспоживання. Наприклад, системи автоматичного вимикання світла та опалення, регулювання температури відповідно до потреб користувачів, моніторинг енергоспоживання та відстеження витрат електроенергії.

6) Розваги: «Розумний» дім може також забезпечувати розваги та комфорт своїм мешканцям. Наприклад, системи домашнього кінотеатру, музичні системи, системи автоматичного відтворення фільмів та телевізійних передач, системи звукового огороження тощо.

7) Відкритість та сумісність: «Розумний» дім повинен бути відкритим та сумісним з різними пристроями та системами, що використовуються в будинку. Це дає можливість мешканцям використовувати різні пристрої та системи, необхідні для них, а також розширювати функціональні можливості свого розумного будинку.

Важливо зазначити, що не всі «розумні» будинки мають всі ці характеристики. Кожен розумний дім може мати свої унікальні особливості та функціональні можливості, в залежності від потреб його мешканців. Однак, загальна мета «розумних» будинків - забезпечити комфорт, безпеку та енергоефективність для своїх мешканців, інтегруючи різні системи в одну інтелектуальну платформу.

«Розумний» дім є складною системою, що складається з багатьох компонентів, включаючи сенсори, датчики, контролери, пристрої зв'язку та програмне забезпечення. Однак, основна ідея полягає в тому, щоб створити інтелектуальну систему, що буде автоматизувати багато рутинних задач та забезпечувати контроль за будинком, надаючи зручність та комфорт його мешканцям.

Одним з ключових компонентів розумного дому є система управління, що забезпечує інтеграцію різних підсистем в одну спільну платформу. Це може бути

здійснено за допомогою різних протоколів зв'язку, таких як Wi-Fi, Bluetooth, ZigBee, Z-Wave та інших. Додатково, інтеграція з додатками для мобільних пристроїв та хмарними сервісами дозволяє мешканцям віддалено керувати своїм будинком та відстежувати його стан.

- ZigBee та Z-Wave - це безпроводової технології мережі, які використовуються в «розумних» будинках для забезпечення зв'язку між різними електронними пристроями та системами. Вони дозволяють створювати мережі з великою кількістю пристроїв, що можуть взаємодіяти один з одним без необхідності використання проводів.

Однією з головних переваг є енергоефективність, що дозволяє пристроям працювати на батарейках протягом довгого часу. Це особливо важливо для розумних будинків, де може бути велика кількість електронних пристроїв, таких як датчики, замки, термостати, світильники та інші, які потребують зв'язку між собою.

ZigBee має високий рівень безпеки та захищеності даних, завдяки застосуванню різноманітних протоколів шифрування та автентифікації. Це дозволяє уникнути кібератак та забезпечити конфіденційність персональних даних власників будинку.

Завдяки технології ZigBee, власники розумних будинків можуть керувати різними електронними пристроями та системами в будинку, використовуючи мобільні пристрої або голосові помічники. Наприклад, вони можуть включати та вимикати світильники, регулювати температуру, відкривати та закривати входні двері та інші пристрої.

У підсумку, технологія ZigBee - це важливий компонент розумного будинку, який забезпечує безпечний та ефективний зв'язок між різними електронними пристроями та системами.

- Bluetooth - це бездротова технологія, яка широко використовується в «розумних» будинках для підключення різних електронних пристроїв до мережі.

Однією з головних переваг технології перед конкурентами Bluetooth - є його висока швидкість передачі даних та низька вартість обладнання, що дозволяє

використовувати її для підключення до мережі різних пристроїв, включаючи смартфони, планшети, навушники, колонки та інші.

Однак, технологія Bluetooth має свої обмеження, зокрема, обмеження на відстань передачі сигналу та максимальну кількість пристроїв, які можуть бути підключені до однієї мережі. Тому, для більш складних та великих розумних будинків, де необхідно підключати багато пристроїв та систем, більш вдалим для використання технології є такі як Zigbee або Z-Wave.

Ще одним важливим компонентом «розумного» дому є сенсорна мережа, яка включає в себе різні типи датчиків, наприклад датчики руху, датчики диму та вуглекислого газу, датчики вологості та температури, датчики освітлення тощо. Ці датчики забезпечують моніторинг різних параметрів довкілля та дозволяють системі автоматично взаємодіяти з різними підсистемами, такими як система опалення, кондиціонування повітря, освітлення тощо

Інші ключові підсистеми розумного дому включають в себе системи безпеки, які забезпечують моніторинг різних входів та вікон, а також системи відеоспостереження, що дозволяють відстежу

Окрім цього, «розумний» будинок може включати і додаткові функції, наприклад:

- Систему безпеки: вона може включати в себе камери відеоспостереження, датчики руху, датчики відкриття вікон та дверей, систему пожежної сигналізації та інші пристрої, які забезпечують безпеку в будинку.
- Автоматизацію освітлення: система «розумного» освітлення дозволяє вмикати та вимикати світло у будь-якій кімнаті, контролювати його яскравість та кольори, а також регулювати освітлення залежно від часу доби та погоди.
- Управління електроприладами: «розумний» будинок може мати систему управління електроприладами, яка дозволяє вмикати та вимикати побутові прилади, налаштовувати їх робочий режим та контролювати споживання електроенергії.

- Систему управління температурою: вона дозволяє автоматично регулювати температуру в будинку, контролюючи роботу опалення та кондиціонування повітря.
- Аудіо та відео системи: «розумний» будинок може мати системи звуку та відео, які дозволяють слухати музику в будь-якій кімнаті, переглядати відеофайли та транслювати медіа контент з інтернету.
- Автоматизовані системи поливу та зрошення: ці системи дозволяють контролювати полив та зрошення рослин на ділянці навколо будинку, регулювати їх роботу та контролювати споживання води.

Іншою важливою характеристикою є застосування штучного інтелекту. «Розумний» дім може використовувати алгоритми машинного навчання та інші методи штучного інтелекту для аналізу даних та покращення ефективності та безпеки.

Також важливою характеристикою є можливість керування будинком з допомогою мобільного пристрою. Завдяки цьому користувач може керувати різними системами в будинку з будь-якого місця з доступом до Інтернету [3].

Нарешті, розумний будинок повинен бути забезпечений захистом від несанкціонованого доступу. Забезпечення кібербезпеки є ключовим аспектом розумного будинку, тому що несанкціонований доступ може призвести до серйозних наслідків, таких як крадіжка даних, витрати електроенергії, викрадення особистої інформації та інші.

1.3 Законодавче регулювання розумних будинків

Законодавче регулювання «розумних» будинків знаходиться у стані постійного розвитку і варіюється в залежності від країни та регіону. Зазвичай, регулювання розумних будинків має на меті забезпечити безпеку, конфіденційність та приватність даних, а також гарантувати сумісність та стандартизацію між пристроями різних виробників.

У деяких країнах, таких як США, ЄС та Канада, існують законодавчі акти, які визначають правила та стандарти для «розумних» будинків.

У США, закон Закон про захист споживачів від онлайн-фальсифікації та крадіжки даних (Consumer Online Privacy and Data Protection Act) містить положення, які регулюють збір та використання даних в «розумних» будинках. У ЄС, загальний регуляторний фреймворк щодо захисту даних - Загальний регламент про захист даних (GDPR) - застосовується до «розумних» будинків, що дозволяє забезпечити конфіденційність даних та приватність користувачів.

Деякі країни також визначають стандарти та протоколи для «розумних» будинків, які повинні дотримуватися виробники обладнання. Наприклад, у ЄС протоколи стандартизовані Європейським інститутом з телекомунікаційних стандартів (ETSI), який відповідає за розробку стандартів телекомунікаційних технологій.

У деяких країнах існують також вимоги щодо включення основних характеристик «розумного» будинку, таких як енергоефективність, безпека та зручність користування, у будівельні стандарти.

У США, крім спеціальних стандартів, законодавче регулювання розумних будинків залежить від законодавства штату, де вони розташовані. У багатьох штатах є закони, які регулюють використання різних технологій у будівлях, таких як будинки, офіси і т.д.

У штаті Каліфорнія був прийнятий закон, який обов'язково вимагає встановлювати зарядні станції для електромобілів у нових будівлях і ремонтіваних будівлях з паркінгом, які мають понад 10 місць для паркування [4].

У Європі законодавство також починає регулювати використання «розумних» технологій у будівництві. Наприклад, в 2020 році Європейський союз прийняв директиву щодо енергоефективності будівель, яка зобов'язує країни-члени забезпечувати, щоб нові будівлі були здатні підключатися до розумних мереж та були обладнані лічильниками енергії, які забезпечують точне вимірювання споживання електроенергії.

Загалом, законодавство різних країн, що регулює «розумні» будинки, ще знаходиться на етапі розробки та уточнення. Оскільки розвиток цієї технології відбувається досить швидко, законодавство повинно адаптуватися до нових вимог і реалій.

Законодавче регулювання розумних будинків ще не є повністю розробленим і у багатьох країнах ще потребує доробки. Однак, деякі законодавчі акти вже були прийняті з метою забезпечення безпеки, приватності та стандартів в розумних будинках.

У США існує закон про безпеку і приватність в Інтернеті речей, який був прийнятий у 2017 році. Згідно з цим законом, виробники розумних пристроїв повинні забезпечити захист від несанкціонованого доступу до даних користувачів та забезпечити можливість зміни паролів та оновлення програмного забезпечення.

У Європейському Союзі також прийнято законодавчі акти, що стосуються розумних будинків та Інтернету речей. Загальний регламент про захист даних (GDPR) встановлює вимоги до збору та обробки персональних даних в «розумних» пристроях та системах.

Україна на даний момент не має окремого законодавства, що стосується регулювання «розумних» будинків, проте законодавство з питань захисту персональних даних та безпеки інформації в цілому також застосовується до «розумних» будинків.

Оскільки технології «розумних» будинків швидко розвиваються, законодавці постійно працюють над оновленням законодавства, щоб забезпечити захист прав та інтересів користувачів розумних будинків.

Цікава інформація заключається в тому, що деякі країни встановлюють стандарти для «розумних» будинків, які регулюють технічні та безпекові вимоги до систем розумного дому. Наприклад, в США і Канаді існують стандарти під назвою Z-Wave та ZigBee, які встановлюють специфікації для «розумних» пристроїв і забезпечують їх сумісність з іншими системами.

У Європі та інших країнах світу також існують стандарти, які регулюють технічні та безпекові вимоги до систем розумного дому. Наприклад, в Європі

існують стандарти EN 50131 та EN 50136, які встановлюють вимоги до систем безпеки будинку, включаючи системи контролю доступу, датчики руху та виклику тривоги.

Україна також регулює використання технологій «розумного» дому. Наприклад, в 2019 році Міністерство енергетики та вугільної промисловості України затвердило Правила встановлення лічильників тепла та регулювання теплових мереж, які вимагають встановлення інтелектуальних лічильників тепла з можливістю зчитування даних за допомогою мережі Інтернет.

Також в Україні існують стандарти Національного стандартизаційного органу Держстандарт України, які регулюють технічні вимоги до електричних пристроїв та систем автоматизації.

Наприклад, стандарт ДСТУ 6110:2010 «Системи автоматизації будинків та будівель» встановлює вимоги до систем автоматизації будинків, включаючи системи освітлення, клімат-контролю та безпеки.

Що стосується міжнародного законодавства, то на даний момент не існує уніфікованих стандартів для розумних будинків. Проте, існують різні директиви та рекомендації, що визначають загальні принципи та вимоги до забезпечення безпеки, захисту даних та приватності в розумних будинках.

Найбільш відомими з них є:

1) Рекомендації з безпеки Інтернету речей (IoT) від Федерального Бюро Зв'язку (FCC) США, які розроблені для захисту споживачів від шкідливих наслідків використання IoT-пристроїв.

2) Рекомендації з захисту даних та приватності від Європейської Комісії (GDPR), які регулюють збір, зберігання та використання особистих даних у розумних будинках.

3) Стандарти безпеки IEC 62443, що регулюють безпеку та захист від кібератак у системах автоматизації та управління промисловими процесами.

4) Стандарти безпеки ISO/IEC 27001, які встановлюють вимоги до систем управління інформаційною безпекою в організаціях.

На національному рівні, кожна країна може мати свої власні законодавчі акти, що регулюють використання розумних будинків. Наприклад, в США була ухвалена «Лейк-Велкомс Передова інтернет-технологія та інновації відповідальності за забезпечення безпеки та приватності» (Lake-View-Wells Advanced Internet Technologies and Innovation Responsibility and Privacy Act), яка ставить перед виробниками IoT-пристроїв вимоги щодо забезпечення безпеки та захисту даних.

Недавні дослідження показали, що існує необхідність у стандартизації технологій, які використовуються в «розумних» будинках, а також в законодавчому регулюванні використання даних, зібраних в розумних домах. У багатьох країнах, включаючи США, Канаду та Європейський Союз, вже були прийняті закони, що регулюють «розумні» будинки та вимагають захисту особистих даних, зібраних в цих системах.

У США було прийнято закон «Закон про захист особистих даних в Інтернеті» (COPPA), який регулює збір та використання інформації про дітей віком до 13 років. Закон також вимагає від операторів веб-сайтів та мобільних додатків отримати згоду батьків на збір даних про дітей [4].

У Європейському Союзі було прийнято загальний регламент про захист даних (GDPR), який став чинним у травні 2018 року. Цей регламент вимагає від організацій отримати згоду користувачів на збір та використання їх персональних даних. Крім того, він надає право користувачам звернутися до органів з питань захисту даних з проханням видалити їх персональні дані.

Також існують стандартизовані протоколи, які використовуються в «розумних» будинках для забезпечення безпеки та обміну даними між різними пристроями та системами. Один з таких протоколів - Z-Wave - розроблений спеціально для використання в розумних будинках та забезпечує стандартизований і безпечний обмін даними між різними пристроями.

«Розумні» будинки, що працюють на основі інтернету речей, є новітнім напрямком розвитку будівництва. Їх можливості вражають своєю широтою та багатофункціональністю, забезпечуючи зручність та комфорт мешканцям.

У майбутньому розумні будинки стануть стандартом життя, а їх використання буде набагато більш поширеним. Прогресуючі технології дозволяють зробити житло більш зручним, безпечним та економічним.

«Розумний» будинок є не тільки модним, але і корисним вкладенням для майбутнього, що може зменшити витрати на комунальні послуги та забезпечити безпеку для вашої родини. Це інвестиція в якість та зручність життя, а також в екологічність.

Висновки до першого розділу

Проведено аналіз поняття та актуальності і важливості «розумний» будинок з використанням обладнання Cisco в наші дні. «Розумний» будинок відноситься до будинку, який використовує автоматизовану систему для керування різними пристроями, електрикою, системами безпеки та комунікацій. Такі будинки дозволяють жителям контролювати та керувати різними пристроями та системами з одного місця, що забезпечує зручність та економію часу.

Досліджено розвиток «розумних» будинків та схеми з контролерами для керування системами в будинку.

Розглянуто основні характеристики «розумного» будинку, які полягають у забезпеченні комфорту, безпеки та ефективності життя, а саме: забезпечення автоматизованого керування електроенергією, освітленням, опаленням, кондиціонуванням повітря, контролю систем безпеки та комунікацій.

2 УПРАВЛІННЯ ТА ОБ'ЄДНАННЯ АВТОМАТИЗОВАНИМИ СИСТЕМАМИ «РОЗУМНОГО» БУДИНКУ

2.1 Використання технологій в «розумному» домі

У «розумному» домі використовуються різні технології, що забезпечують його роботу та зв'язок між різними пристроями та системами. Ось деякі з найпоширеніших технологій, що використовуються в розумних будинках:

- 1) Wi-Fi - це бездротова технологія зв'язку, яка забезпечує швидкий та стабільний доступ до Інтернету у всьому будинку.
- 2) Bluetooth - це технологія бездротового зв'язку короткого радіусу, що використовується для з'єднання між різними пристроями, такими як смартфони, навушники, динаміки та інші.
- 3) Zigbee - це бездротова технологія зв'язку, що використовується для зв'язку між різними "розумними" пристроями в будинку, такими як датчики руху, датчики вогню та інші.
- 4) Z-Wave - це ще одна бездротова технологія зв'язку, яка використовується для керування різними пристроями в будинку, такими як освітлення, опалення, система безпеки та інші.
- 5) NFC - це технологія близького бездротового зв'язку, яка дозволяє обмінюватися даними між двома пристроями, просто зближуючи їх один з іншим.
- 6) Інфрачервона технологія - це технологія, що використовується для керування пристроями, такими як телевізори, кондиціонери, системи аудіо та інші.
- 7) Cloud-технології - це технології, що дозволяють зберігати дані в хмарі та керувати різними пристроями в будинку з будь-якого місця з доступом до Інтернету.

Крім технологій, згаданих вище, в «розумних» будинках також можуть використовуватися різноманітні датчики, зокрема датчики руху, температури, вологості, якості повітря, а також датчики вікон і дверей. Ці датчики допомагають

збирати інформацію про стан будинку та його мешканців, що може бути використано для вдосконалення системи управління.

Однією з ключових технологій, що використовується в «розумних» будинках, є Інтернет речей (IoT). IoT дозволяє підключати до мережі Інтернет різноманітні пристрої, такі як датчики, електроприлади, системи безпеки, системи опалення та кондиціонування повітря. Це дозволяє дистанційно керувати всіма цими пристроями через Інтернет, що забезпечує високу рівень комфорту та енергоефективності.

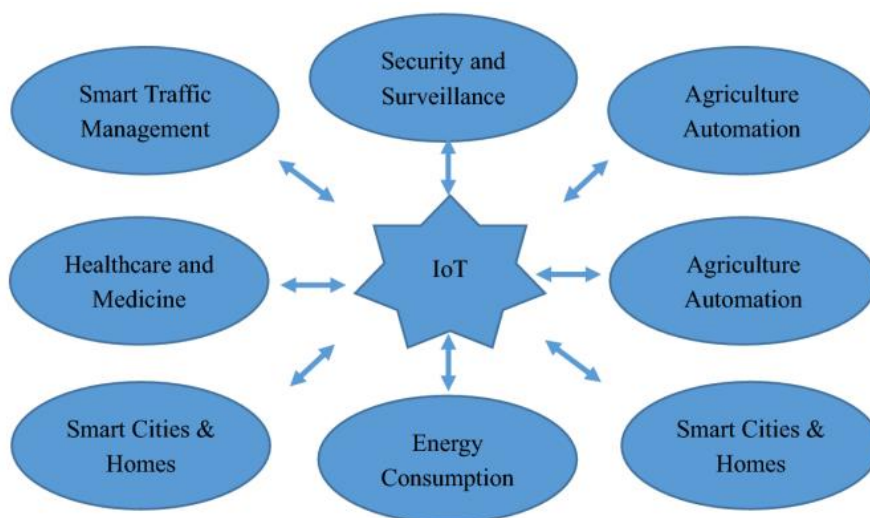


Рис.2.1. Потенційні області застосування Інтернет речей

Крім того, в «розумних» будинках можуть використовуватися системи штучного інтелекту, що дозволяють аналізувати інформацію, зібрану датчиками та іншими пристроями, та приймати рішення щодо управління будинком. Такі системи можуть навіть навчатися на основі досвіду та історії використання пристроїв у будинку та управляти їх роботою відповідно їх енергоспоживання та ефективного управління. Блокчейн також може допомогти забезпечити безпеку даних, збережених у системі управління будинком, оскільки він дозволяє зберігати дані в зашифрованому вигляді та контролювати доступ до них.

Важливим елементом «розумного» будинку є також системи зберігання енергії, які можуть забезпечувати енергонезалежність та допомагати економити на витратах на електроенергію. Серед технологій, що використовуються для

зберігання енергії, можна виділити сонячні батареї, батареї зарядки на основі вітроенергії та гідроенергії, а також системи зберігання енергії на основі різних хімічних речовин.

Остаточню, важливо зазначити, що «розумні» будинки – це дуже комплексна система, яка поєднує в собі різноманітні технології та пристрої. Ці технології дозволяють забезпечити високий рівень комфорту, енергоефективності та безпеки у будинку, що робить їх дуже привабливими для власників житла та інших користувачів.

Зокрема, що стосується систем автоматизації, то вони базуються на інтернеті речей (IoT), який дозволяє розумним пристроям спілкуватись між собою та зі спеціальними платформами керування. Наприклад, система освітлення може виконувати різні функції, такі як включення світла відповідно до розкладу, адаптування яскравості до зміни освітленості в приміщенні, включення світла відповідно до наявності людей у кімнаті тощо. Аналогічні функції реалізуються у системах опалення, кондиціонування повітря та інших.

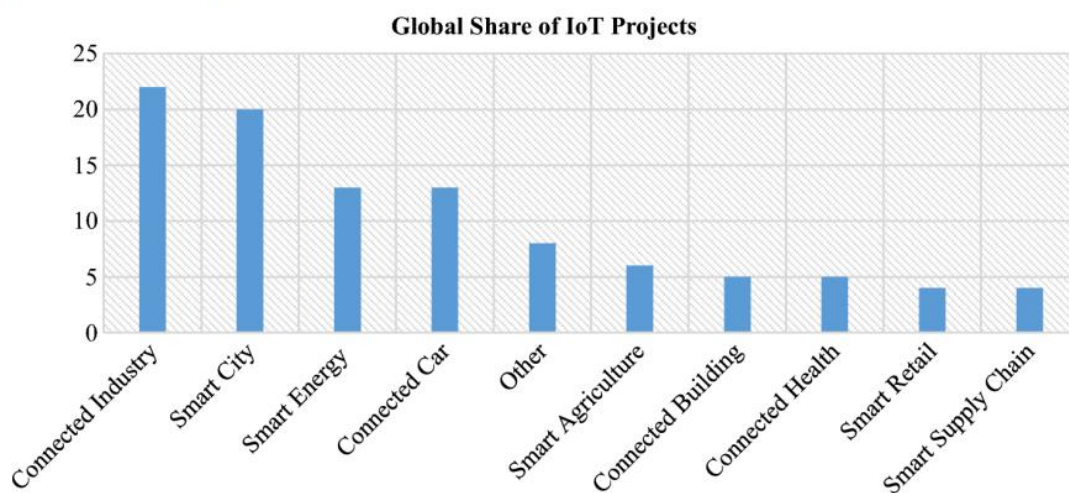


Рис.2.2. Глобальна частка проектів Інтернет речей

Також важливими елементами «розумного» будинку є системи безпеки. Вони можуть включати в себе різні пристрої, такі як відеорекамери, датчики руху, сигналізацію тощо. Важливою частиною таких систем є аналіз даних, зібраних датчиками, який дозволяє здійснювати швидке та ефективне реагування на небезпеку.

У «розумному» будинку також можуть використовуватися системи звуку та відео, що дозволяють користувачам насолоджуватися якісним звуком та відео у різних кімнатах. Такі системи можуть включати в себе вбудовані динаміки, які можуть зв'язуватися між собою, а також з музичними сервісами через інтернет.

Іншою важливою складовою «розумного» будинку є системи автоматичного керування водопостачанням та каналізацією. Такі системи можуть дозволяти оптимізувати витрати води, контролювати рівень води в баках, а також управляти роботою насосів та інших пристроїв.

Інші технології, що використовуються в «розумних» будинках, це різноманітні датчики. Датчики дозволяють зчитувати різні параметри навколишнього середовища, такі як температура, вологість, освітленість і якість повітря. З цими даними система управління розумним будинком може аналізувати та керувати різними системами будинку, зокрема опаленням, вентиляцією, кондиціонуванням повітря і освітленням.

Ще однією важливою технологією, що використовується в «розумних» будинках, є технології збереження та управління енергією. Наприклад, системи управління енергопотоками можуть оптимізувати використання електроенергії в будинку, знижуючи споживання та забезпечуючи економію енергоресурсів. Також «розумний» будинок може використовувати сонячні батареї для збору сонячної енергії та забезпечення електропостачання будинку [4].

Залежно від конфігурації «розумного» будинку, можуть використовуватися й інші технології, такі як системи безпеки (наприклад, камери відеоспостереження та датчики диму), системи зв'язку (наприклад системи домашнього кінотеатру) та інші.

2.2 Обладнання Cisco та його особливості

Cisco - це провідний світовий виробник обладнання для мережевих технологій, включаючи технології для «розумних» будинків. Вони пропонують

різні рішення для розумних будинків, включаючи мережеве обладнання, роутери, комутатори, маршрутизатори, контролери мережі та інші рішення.

Однією з основних особливостей обладнання Cisco є його здатність працювати в режимі реального часу, що дозволяє швидко реагувати на зміни у середовищі та забезпечувати безперебійну роботу розумного дому. Крім того, Cisco пропонує зручні інтерфейси управління, що дозволяють користувачам легко налаштовувати та контролювати свої «розумні» будинки.

Іншою важливою особливістю обладнання Cisco є його висока надійність та безпека. Cisco пропонує багато інструментів безпеки, включаючи фірмові рішення, такі як Cisco Security Manager та Cisco Identity Services Engine. Ці інструменти забезпечують захист від кібератак та інших загроз безпеки, що можуть загрожувати розумному дому.

Крім того, обладнання Cisco є досить гнучким та може інтегруватись з різними іншими пристроями та технологіями для «розумних» будинків. Це дозволяє користувачам легко розширювати та модернізувати свій розумний дім, щоб задовольняти змінні потреби та вимоги.

Загалом, обладнання Cisco є надійним та безпечним рішенням для «розумного» дому, здатним працювати в реальному часі та інтегруватись з іншими пристроями та технологіями для розумних будинків.

Однією з особливостей обладнання Cisco є його гнучкість і масштабованість. Cisco пропонує широкий спектр рішень для «розумного» будинку, що можуть бути легко налаштовані та збільшені в залежності від потреб користувачів.

Крім того, обладнання Cisco забезпечує високу надійність і безпеку систем «розумного» будинку. Він використовує передові технології захисту, такі як захист від вторгнень, аутентифікація користувачів і шифрування даних.

Також важливою особливістю обладнання Cisco є можливість інтеграції з іншими пристроями та системами «розумного» будинку, що дозволяє користувачам створювати повноцінні та інтелектуальні системи управління будинком.

У загальному, обладнання Cisco забезпечує не тільки надійність та безпеку «розумного» будинку, але й дозволяє користувачам з легкістю керувати будинком за допомогою мобільних пристроїв та інтернету з будь-якого місця світу.

Окремим аспектом використання обладнання Cisco у «розумному» будинку є можливість забезпечення безпеки мережі та даних, що пересилаються між пристроями. Виробник пропонує широкий асортимент рішень для забезпечення цього аспекту, зокрема брандмауери, інтегровані системи захисту від вторгнень, VPN-сервери, системи ідентифікації та автентифікації користувачів, а також системи контролю доступу до мережевих ресурсів.

Додатковою перевагою використання обладнання Cisco є можливість моніторингу та керування всіма пристроями мережі з централізованої точки управління. Це дозволяє швидко виявляти та вирішувати проблеми у мережі, налаштовувати та оптимізовувати роботу пристроїв.

У «розумному» будинку обладнання Cisco може використовуватись для підключення різних пристроїв та систем, таких як системи безпеки, відеоспостереження, освітлення, опалення та кондиціонування повітря. За допомогою спеціального програмного забезпечення та протоколів зв'язку (наприклад, протоколу Internet of Things MQTT), ці системи можуть взаємодіяти між собою та здійснювати автоматичне керування на основі зібраних даних.

Саме тому використання обладнання Cisco у «розумному» будинку дозволяє забезпечити надійність та безпеку мережі, забезпечити її масштабованість та зручність управління, а також забезпечити взаємодію між різними системами та пристроями, що є ключовим аспектом для створення повноцінного «розумного» будинку.

Таким чином, обладнання Cisco є однією з ключових технологій, які використовуються у «розумних» будинках. Завдяки своїм особливостям, таким як висока швидкість передачі даних, висока надійність та масштабованість, обладнання Cisco дозволяє забезпечувати безперебійну роботу систем управління будинком, забезпечувати безпеку та зручність для користувачів.

Однією з найбільш важливих особливостей обладнання Cisco є його можливість працювати у великих мережах. Це дозволяє об'єднувати в собі різноманітні системи будинку, такі як освітлення, опалення, кондиціонування повітря, безпека та інші, та управляти ними з одного центрального пункту. Це зроблює систему управління будинком більш ефективною та зручною в експлуатації.

Крім того, обладнання Cisco має високий рівень безпеки, що є особливо важливим для «розумних» будинків, де забезпечення безпеки є однією з ключових функцій. Обладнання Cisco включає в себе різноманітні механізми захисту, такі як файрволи, ідентифікацію користувачів, шифрування даних та інші.

Обладнання Cisco має високий рівень масштабованості, що дозволяє розширювати систему управління будинком при необхідності та додавати нові функції без значного збільшення витрат на обслуговування.

Для побудови «розумного» будинку з використанням обладнання Cisco необхідно враховувати ряд особливостей [5]:

- По-перше, обладнання Cisco має високу ціну, тому вартість розумного будинку з використанням такого обладнання може бути високою. Проте, це компенсується високою якістю, масштабованістю та безпекою мережі.
- По-друге, важливо мати професійну команду зі знанням мережевих технологій Cisco, яка зможе правильно налаштувати мережу відповідно до потреб користувача. Така команда зможе забезпечити безпеку мережі, зменшити ризик збоїв, а також забезпечити максимальну продуктивність мережі.
- По-третє, обладнання Cisco має високі технічні характеристики, що дозволяє забезпечити високу швидкість передачі даних та стабільну роботу мережі. Також воно має широкий спектр можливостей для інтеграції з іншими системами та пристроями.

Важливо зазначити, що обладнання Cisco відповідає всім необхідним стандартам безпеки, що дозволяє запобігти злому мережі та викраденню конфіденційної інформації. Безпека важлива, особливо у «розумному» будинку, де кількість підключених пристроїв може бути значною.

2.3 Аналіз можливостей обладнання Cisco для створення розумного дому

Обладнання Cisco має широкі можливості для створення «розумного» дому. Наприклад, відомий продукт Cisco Smart Home Automation пропонує повністю інтегрований підхід до управління різними пристроями та системами в «розумному» домі. Ця система забезпечує керування освітленням, опаленням, кондиціонуванням повітря, безпекою та іншими функціями за допомогою одного центрального контролера.

Cisco Smart Home Automation - це програмне забезпечення для управління розумним домом, яке забезпечує інтеграцію різних пристроїв та технологій в одну систему керування. Ця система може бути використана для автоматизації основних функцій в домі, таких як освітлення, опалення, кондиціонування повітря, безпека та зв'язок.



Рис.2.3. Візуалізована частина можливостей CSHA

CSHA є однією з ключових технологій, яка дозволяє створити «розумний» дім з використанням обладнання Cisco. Ця технологія дозволяє об'єднати різні

елементи розумного дому в єдину систему керування, яка забезпечує автоматизацію роботи пристроїв та оптимізацію енергоспоживання.

Cisco Smart Home Automation базується на технології Internet of Things (IoT) та мережі Wi-Fi, що забезпечує з'єднання різних пристроїв і систем у розумну мережу, яку можна керувати за допомогою мобільного додатку або голосових команд.

Однією з ключових особливостей Cisco Smart Home Automation є гнучкість та можливість розширення. Це означає, що систему можна налаштувати під будь-які потреби користувача та додавати до неї нові пристрої з часом. Крім того, система може інтегруватися з іншими платформами та системами для забезпечення ще більшого рівня автоматизації та керування.

Основні можливості CSHA (Cisco Smart Home Automation) включають в себе наступні функції:

1. Керування освітленням та термостатами. За допомогою цієї технології можна налаштувати автоматичне включення та вимикання освітлення, а також налаштувати термостати, щоб забезпечити оптимальну температуру в будинку.
2. Керування системами безпеки. За допомогою Cisco Smart Home Automation можна контролювати системи безпеки, такі як камери відеоспостереження, датчики руху та системи доступу до приміщення.
3. Керування аудіо та відеосистемами. За допомогою цієї технології можна налаштувати автоматичне включення та вимикання аудіо- та відеообладнання, а також керувати звуковими та відеоустройствами з будь-якого місця в будинку.
4. Керування енергоспоживанням. Cisco Smart Home Automation дозволяє контролювати споживання електроенергії та води, що дозволяє економити кошти на оплату рахунків.
5. Інтеграція з голосовими помічниками. Технологія Cisco Smart Home Automation може бути інтегрована з голосовими помічниками, такими як Amazon Alexa чи Google Assistant, що дозволяє керувати «розумним» домом голосом.

Обладнання від компанії Cisco, пропонує можливості для віддаленого керування «розумним» будинком. Для цього можна використовувати мобільні додатки, які дозволяють керувати різними функціями «розумного» дому з будь-якої точки світу, де є доступ до Інтернету.

Також обладнання Cisco має великий вибір протоколів зв'язку, які дозволяють інтегрувати різноманітні пристрої та системи в «розумний» дім.

Високий рівень безпеки для «розумного» дому зумовлений тим, що мережеві пристрої Cisco мають вбудовані засоби захисту від хакерських атак та вірусів.

Cisco є одним з провідних постачальників технологій Internet of Things (IoT). Їхній підхід до IoT базується на тому, що вони надають повністю інтегровану систему для створення розумних мереж. Вони пропонують низку продуктів та рішень, що допомагають впроваджувати IoT-технології у різних сферах, включаючи «розумний» дім.

Одним з головних продуктів Cisco для IoT є Cisco Kinetic. Це програмне забезпечення для збору даних, їхньої аналітики та управління різними IoT-пристроями. За допомогою Cisco Kinetic можна зібрати дані від різних датчиків та пристроїв, а потім обробити їх за допомогою аналітики даних, щоб зробити рішення щодо управління мережею.

Cisco також пропонує різні пристрої та рішення для побудови «розумних» мереж. Наприклад, Cisco Smart Wi-Fi є рішенням для створення бездротової мережі, яке дозволяє управляти інтернет-підключенням та іншими параметрами мережі за допомогою спеціальної програми. Крім того, Cisco також пропонує різні рішення для управління світлом, опаленням, кондиціонуванням повітря та іншими системами у «розумному» домі [6].

Однією з особливостей Cisco є те, що вони ставлять на перше місце питання безпеки мережі. Вони пропонують рішення для захисту мережі від зломів та хакерських атак, що є дуже важливим для «розумних» мереж. Також вони мають платформу для моніторингу та аналізу безпеки мережі, що дозволяє виявляти загрози та уразливості у режимі реального часу.

2.4 Вибір обладнання та технологій для створення «розумного» дому з використанням обладнання Cisco

Вибір обладнання та технологій для створення «розумного» дому з використанням обладнання Cisco може бути складним завданням, оскільки він залежить від конкретних потреб та бюджету. Однак, компанія Cisco пропонує широкий вибір продуктів, які можуть використовуватися в «розумних» домах.

Основні продукти Cisco, які можуть бути використані для створення «розумного» дому, включають:

1. Cisco Smart Home Automation. Це рішення, що дозволяє створювати «розумний» дім за допомогою мережі Cisco. Це рішення включає в себе мережеві пристрої, які можуть бути підключені до різних пристроїв в домі, таких як «розумні» термостати, системи освітлення та безпеки. Також, рішення Cisco Smart Home Automation дозволяє керувати різними пристроями з одного місця, що робить його дуже зручним та ефективним.

2. Cisco Meraki. Це спосіб, який дозволяє керувати мережею в «розумному» домі з одного місця. Це може бути особливо корисно для великих розумних домів або комплексів. Cisco Meraki дозволяє керувати інтернет-з'єднанням, мережевим обладнанням та захистом мережі.

3. Cisco Wireless. Бездротова мережа є ключовим елементом «розумного» дому. Cisco пропонує широкий вибір бездротових пристроїв, які можуть бути використані для підключення до різних пристроїв в домі, таких як телефони, планшети та комп'ютери. Вони також можуть бути використані для підключення до різних «розумних» пристроїв, таких як розумні термостати та системи освітлення.

4. Cisco Kinetic for Cities. Даний продукт дозволяє містам та регіонам віддалено керувати мережами вуличного освітлення, системами контролю трафіку, датчиками повітряної якості та іншими IoT-рішеннями. Він також надає інструменти для збору, аналізу та використання даних з цих систем для забезпечення більш ефективного та економічного керування містом.

5. Cisco Jasper Control Center. Цей продукт дозволяє забезпечити підключення мільйонів IoT-пристроїв до хмарної інфраструктури та керувати ними за допомогою мережевого протоколу MQTT. Він надає інструменти для керування підключенням, моніторингу та діагностики IoT-пристроїв, а також для створення та керування послугами, пов'язаними з IoT.

6. Cisco DNA Center. Продукт дозволяє керувати мережею та IoT-пристроями з одного місця. Він надає інтегровану платформу для керування мережевою інфраструктурою, IoT-пристроями та безпекою. Для керування IoT-пристроями, що працюють на платформі Cisco Kinetic, Cisco DNA Center надає можливості збору даних, аналізу та керування IoT-пристроями в реальному часі.

7. Cisco Security. Це сімейство рішень для забезпечення безпеки мережі. Воно включає в себе пристрої для брандмауерів, обмеження доступу до мережі, виявлення загроз та багато іншого. Ці рішення можуть бути використані для забезпечення безпеки розумного дому та його мережі.

- **Cisco Meraki** - це інтернет-платформа, що надається компанією Cisco Systems для керування мережами Wi-Fi, мережевої безпеки, комутації, моніторингу відео та інших різноманітних мережевих рішень. Ця платформа дозволяє забезпечити безпеку та надійність мережі, а також спростити її управління.



Рис.2.4. Логотип Cisco Meraki

Cisco Meraki працює на основі хмарної технології, що дозволяє забезпечувати управління мережею з будь-якого місця, де є доступ до інтернету. Це дає можливість адміністраторам мережі віддалено налаштовувати та моніторити

мережеві пристрої, стежити за безпекою мережі, відслідковувати трафік та аналізувати дані про використання мережі.

Основні переваги Cisco Meraki включають:

- Простоту установки та налаштування пристроїв;
- Швидкість та надійність мережі;
- Високий рівень безпеки та захисту мережі від загроз ззовні;
- Зручну віддалену підтримку та управління мережею;
- Автоматичне оновлення програмного забезпечення та підтримка нових технологій.

Cisco Meraki використовують у різних сферах, включаючи бізнес, освіту, організації громадського харчування та багатоквартирні будинки. Дана технологія дозволяє значно полегшити управління мережею та забезпечити її безпеку та надійність.

Вона також надає також додаткові можливості для аналізу та оптимізації мережі. Забезпечення збору даних про використання мережі, що дозволяє аналізувати дані про трафік та використання ресурсів мережі. Це може допомогти адміністраторам мережі приймати рішення про зміни у налаштуванні мережі, що дозволить підвищити її продуктивність та ефективність [7].

Окрім цього, Cisco Meraki має широкі можливості для інтеграції з іншими рішеннями та сервісами. Наприклад, її можна інтегрувати з системами контролю доступу, системами електронних платежів, системами управління пристроями та іншими системами. Це дозволяє створювати комплексні рішення для управління різними процесами у будь-якій організації.

- **Cisco Wireless** є комплексною системою, що надає можливості для забезпечення бездротового зв'язку в приміщенні або на відкритому просторі. Ця технологія дозволяє створювати бездротові мережі з великою швидкістю передачі даних і надійністю зв'язку.

Cisco Wireless має різноманітні можливості, серед яких:

A. Мережева інфраструктура для бездротових мереж: Cisco Wireless дозволяє створювати бездротові мережі різної конфігурації в залежності від потреб

користувача. Мережева інфраструктура включає в себе точки доступу, контролери мережі, обладнання для моніторингу та керування мережею.

В. Розширені можливості бездротового зв'язку: Cisco Wireless підтримує різноманітні технології бездротового зв'язку, такі як Wi-Fi, Bluetooth, Zigbee, LoRaWAN і інші. Це дозволяє підключати різноманітні пристрої до бездротової мережі і забезпечувати зв'язок між ними.

С. Керування бездротовою мережею: Cisco Wireless надає можливості для керування мережею, включаючи моніторинг мережі, налаштування точок доступу, управління політиками безпеки та доступу до мережі.

Д. Безпека: Cisco Wireless забезпечує високий рівень безпеки мережі, включаючи шифрування даних, автентифікацію користувачів, мережеві файрволи та інші технології захисту.

Таким чином, Cisco Wireless є відмінним вибором для створення «розумного» дому, якщо потрібен надійний та ефективний мережевий доступ з використанням технологій Wi-Fi. Ця технологія дозволяє підключати до мережі різноманітні пристрої, включаючи розумні датчики, камери, термостати та інші, що використовуються в «розумному» домі. Крім того, Cisco Wireless забезпечує бездротовий доступ до Інтернету, що є дуже важливим для роботи різноманітних додатків та сервісів, що використовуються в розумному домі.

Однією з найбільш привабливих можливостей Cisco Wireless є його підтримка технології мережі Mesh, яка дозволяє створювати бездротові мережі без необхідності використання кабелів Ethernet. Це особливо корисно для створення «розумного» дому, де може бути багато різних пристроїв, які потребують доступу до Інтернету. З допомогою технології Mesh можна створити надійну і швидко мережу, яка забезпечує безперебійний доступ до Інтернету в будь-якому куточку будинку.

Cisco Wireless має можливість управління даними з різних точок доступу, що дозволяє адміністраторам мережі контролювати доступ до Інтернету і забезпечити максимальний рівень безпеки. За допомогою цієї технології можна також налаштувати різні режими роботи мережі, такі як гостьова мережа, де гості можуть

отримати доступ до Інтернету, не маючи доступу до внутрішньої мережі. Також вона дозволяє налаштовувати різні параметри мережі, такі як мережевий трафік, пропускну здатність, час доступу до Інтернету і багато іншого. Це дає можливість користувачам мережі регулювати швидкість і якість доступу до Інтернету в залежності від своїх потреб і запитів.

Загалом дана технологія - є потужним і універсальним інструментом для створення розумного дому. Він дозволяє створювати швидку і надійну бездротову мережу, яка забезпечує доступ до Інтернету в будь-якому куточку будинку і контролюється за допомогою централізованої системи управління.

Основними можливостями Cisco Wireless є:

- Підтримка технологій Wi-Fi 6 та Wi-Fi 5 для забезпечення високої швидкості та безпеки бездротового зв'язку;
- Підтримка різноманітних протоколів та стандартів бездротового зв'язку, таких як 802.11ax, 802.11ac, 802.11n, 802.11g, 802.11b та 802.11a;
- Автоматичне керування мережею з використанням технології Cisco DNA Center, що дозволяє забезпечувати безпеку та ефективність мережі за допомогою інтелектуальних аналітичних інструментів;
- Підтримка мережевих пристроїв з функцією IoT, таких як Cisco Catalyst IE3x00 Rugged Series та Cisco IR1101 Integrated Services Router, що забезпечують безпеку та надійність для підключення розумних пристроїв;
- Підтримка різних методів автентифікації, таких як WPA3, 802.1x та інших, що забезпечують безпеку мережі та підключених пристроїв;
- Інтеграція з різноманітними додатками та сервісами, такими як Cisco DNA Spaces, Meraki Dashboard.
- **Cisco Kinetic for Cities** є платформою Internet of Things (IoT), яка дозволяє містам збирати, аналізувати та використовувати дані з різноманітних джерел для управління міською інфраструктурою та послугами.

Cisco Kinetic for Cities Solution Architecture

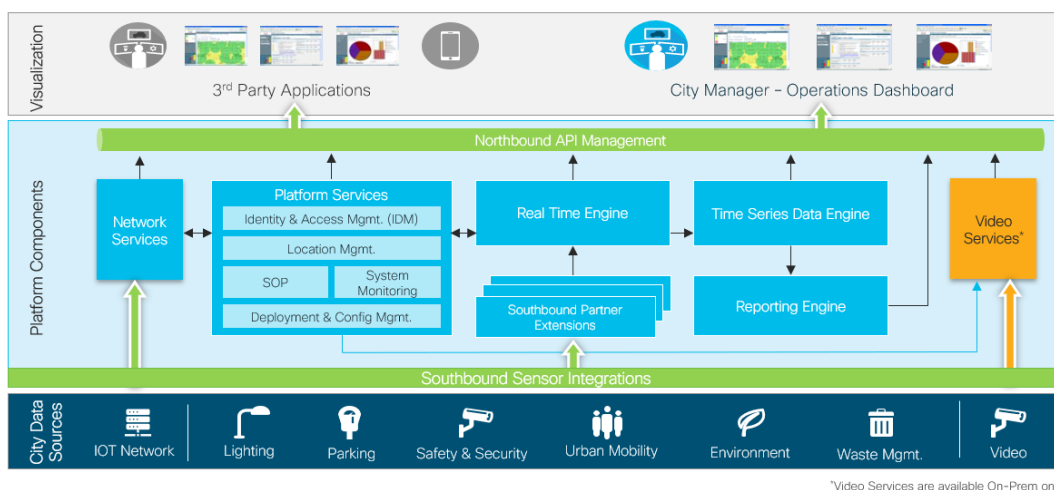


Рис.2.5. Схема архітектури платформи

Це рішення розроблене з урахуванням потреб міст, забезпечуючи зручний та ефективний інтерфейс для відображення та аналізу даних.

Одним з основних компонентів Cisco Kinetic for Cities є система збору даних, яка дозволяє збирати дані з різноманітних джерел, таких як датчики, мережі електронного обміну даними та інші IoT-пристрої. Ці дані передаються на платформу Kinetic for Cities для подальшого аналізу та використання.

Окрім системи збору даних, Cisco Kinetic for Cities також містить інші компоненти, такі як система аналізу даних, система управління даними та система відображення даних. Завдяки цим компонентам, платформа забезпечує збір та аналіз даних, що дозволяє містам більш ефективно управляти своєю інфраструктурою та послугами [8].

Cisco Kinetic for Cities дозволяє містам використовувати дані для управління різноманітними аспектами життя в містах, такими як транспорт, енергетика, водопостачання, освіта та здоров'я. Завдяки збору та аналізу даних, міста можуть виявити проблеми та покращити рівень життя своїх мешканців.

- **Cisco Jasper Control Center (CCC)** - це платформа для управління IoT, яка дозволяє підприємствам забезпечити віддалений доступ, контроль та

управління з'єднаними пристроями та рішеннями, в тому числі транспортними засобами, пристроями "розумного дому", телефонами, планшетами та іншими.

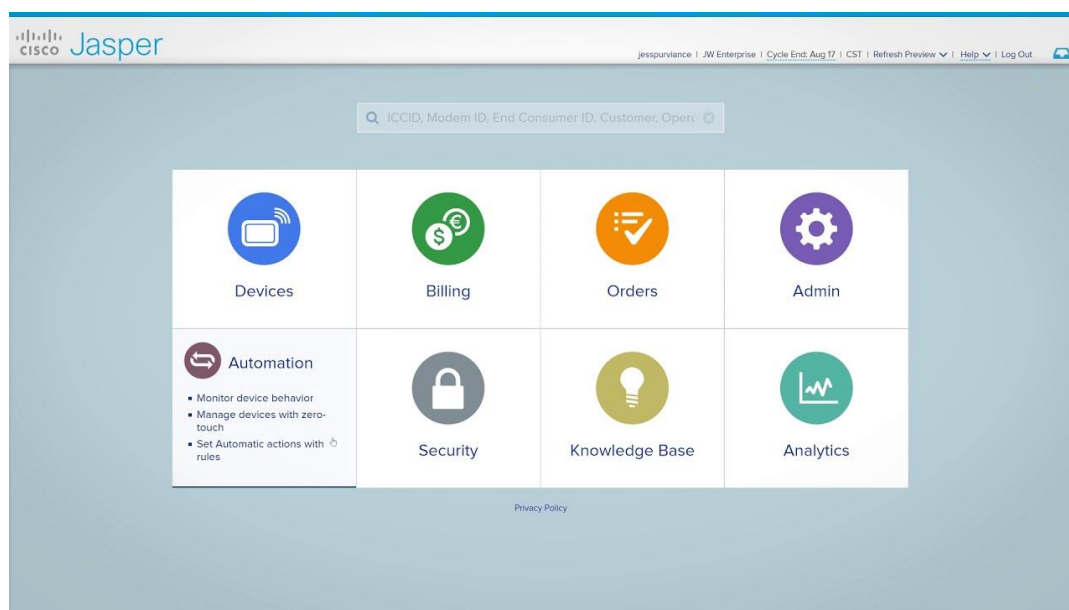


Рис.2.6. Схема платформи CCC

ССС пропонує широкий набір функцій, які дозволяють підприємствам легко взаємодіяти з мільйонами пристроїв, що підключені до мережі IoT, в тому числі віддалено керувати та моніторити ці пристрої. Платформа включає в себе інструменти для створення та налаштування пристроїв, контролю трафіку даних, забезпечення безпеки, аналізу даних та багато іншого.

Завдяки CCC підприємства можуть ефективно використовувати дані, що збираються з пристроїв, для покращення бізнес-процесів, зниження витрат, підвищення якості обслуговування та інноваційного розвитку. Крім того, CCC забезпечує підприємства безпекою, захистом від кібератак та конфіденційністю даних, що збираються з IoT-пристроїв.

Ця хмарна платформа, яка надає компаніям можливість керувати підключеними IoT-пристроями з усього світу. Платформа дозволяє налаштовувати, моніторити та керувати підключеними пристроями через єдиний веб-інтерфейс.

Cisco Jasper Control Center пропонує широкий спектр можливостей для керування IoT-пристроями, включаючи моніторинг стану пристроїв, налаштування

параметрів зв'язку, віддалене керування пристроями, аналіз даних про використання мережі та відслідковування місцезнаходження пристроїв.

Особливість Cisco Jasper Control Center полягає в тому, що вона дозволяє забезпечити безпеку та надійність IoT-пристроїв, що є особливо важливим для розумного будинку, де забезпечення безпеки має вирішальне значення. Платформа включає функції аутентифікації, шифрування та моніторингу безпеки, які допоможуть забезпечити безпеку даних та знизити ризики виникнення кібератак на систему розумного будинку.

Застосування Cisco Jasper Control Center дозволяє забезпечити цілісність та безпеку IoT-пристроїв у системі розумного будинку, зменшуючи ризики витоку конфіденційної інформації та забезпечуючи ефективне керування підключеними пристроями.

- **Cisco DNA Center** - це програмне забезпечення, яке дозволяє керувати мережею компанії та автоматизувати її процеси. Він надає інтегрований підхід до управління мережею, що дозволяє розглядати її як єдину систему, забезпечуючи зручну та централізовану адміністрацію.

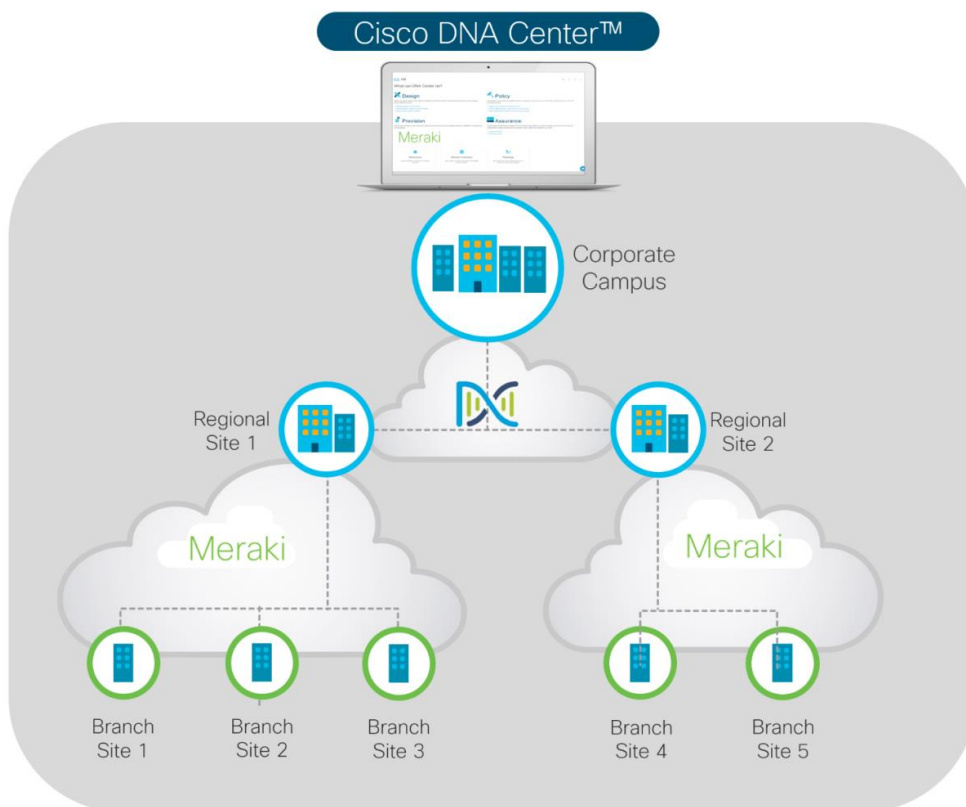


Рис.2.7. Схема архітектури DNA Center

Cisco DNA Center надає такі можливості [9]:

- a) Моніторинг та аналіз мережі: збір даних про пристрої та трафік в режимі реального часу, аналіз мережі, ідентифікація проблем та пропозиції щодо їх вирішення.
- b) Автоматизація мережевих процесів: Cisco DNA Center дозволяє автоматизувати процеси конфігурування, моніторингу та управління мережею.
- c) Керування безпекою: Cisco DNA Center забезпечує централізований контроль над безпекою мережі та дозволяє виявляти та запобігати загрозам.
- d) Інтеграція з різноманітними пристроями: Cisco DNA Center підтримує різноманітні пристрої, такі як маршрутизатори, комутатори, точки доступу та інші, що дозволяє створювати єдину мережеву інфраструктуру.
- e) Аналітика та рекомендації: Cisco DNA Center надає аналітику даних мережі та пропонує рекомендації щодо її покращення.

Ці можливості дозволяють підприємствам управляти мережами більш ефективно, зменшувати час та затрати на їх обслуговування та забезпечувати високий рівень безпеки мережі. Це централізована платформа для керування мережею, яка дозволяє автоматизувати процеси налаштування, моніторингу та управління мережею. Вона надає можливість адміністраторам мережі зосередитись на стратегічних завданнях, забезпечує розширення та підтримку мережі, зменшує час на реакцію на проблеми мережі, забезпечує безпеку мережі та багато іншого.

Плюси використання Cisco DNA Center:

- Централізоване керування: Cisco DNA Center дозволяє керувати всіма компонентами мережі з одного місця, що дозволяє зменшити час та зусилля на налаштування, моніторинг та управління мережею.
- Автоматизація: Cisco DNA Center дозволяє автоматизувати процеси налаштування та управління мережею, що зменшує час та зусилля на їх виконання.
- Аналіз та моніторинг: Cisco DNA Center забезпечує аналіз та моніторинг мережі, що дозволяє адміністраторам мережі оперативно реагувати на проблеми та забезпечувати їх ефективне вирішення.

- Безпека мережі: Cisco DNA Center дозволяє забезпечити безпеку мережі шляхом ідентифікації та відстеження загроз, а також налаштування політик безпеки.
- Інтеграція з іншими продуктами Cisco: Cisco DNA Center інтегрується з іншими продуктами Cisco, такими як Cisco Identity Services Engine (ISE), що дозволяє забезпечити безпеку мережі та управління доступом.
- Віддалене керування: Cisco DNA Center дозволяє керувати мережею з будь-якого місця, що забезпечує зручність та ефективність управління.
- **Cisco Security** є однією з найбільш сучасних та надійних систем безпеки, яка використовується у різних галузях, включаючи «розумний» дім. Вона забезпечує комплексний захист від різноманітних кіберзагроз, що можуть призвести до витоку конфіденційної інформації та відключення мережі.



Рис.2.8. Візуалізація платформеного підходу безпеки з Cisco Security(X)

Система Cisco Security включає в себе різноманітні засоби захисту, такі як мережеві брандмауери, системи виявлення та запобігання вторгненням, системи аутентифікації та авторизації користувачів, системи контролю доступу до мережевих ресурсів тощо. Крім того, вона підтримує стандарти безпеки, такі як SSL, IPSec, WPA, WPA2, а також вмонтовані захисти від DDoS-атак.

Cisco Security дозволяє забезпечувати безпеку як окремих пристроїв, так і всієї мережі в цілому. Завдяки цьому, власники «розумних» будинків можуть бути

впевнені в тому, що їхні пристрої та системи не піддаються кібератакам, а їхні дані залишаються захищеними [10].

Cisco Security є однією з ключових гілок компанії Cisco, яка пропонує широкий спектр рішень для забезпечення безпеки мережі та захисту інформації. Ці продукти та рішення допомагають уникнути загроз безпеці, забезпечуючи відстеження та захист від шкідливих програм, витоку даних та інших видів кібератак.

Cisco Security пропонує такі продукти та рішення:

- Cisco Umbrella - хмарна безпека, яка дозволяє захистити користувачів від шкідливих сайтів, доменів та IP-адрес.
- Cisco Identity Services Engine (ISE) - рішення для контролю доступу та автоматизації політик безпеки в мережах.
- Cisco Adaptive Security Appliance (ASA) - брандмауер з інтегрованою системою захисту від загроз та забезпеченням приватності.
- Cisco Stealthwatch - система моніторингу безпеки, яка дозволяє відстежувати аномальну активність у мережі та запобігати кібератакам.
- Cisco Firepower - рішення для захисту від загроз, яке включає в себе брандмауер, IPS, систему захисту від шкідливого ПЗ та інші інструменти.

Ці продукти та рішення допомагають захистити мережу та забезпечити безпеку даних в розумному домі, забезпечуючи захист від кібератак та інших загроз безпеці.

Висновки до другого розділу

Досліджено технології, що використовуються в «розумному» домі, переваги та недоліки такої системи, законодавче регулювання щодо її використання, а також було описано обладнання Cisco та його особливості.

Проаналізовано технології, що використовуються в «розумному» домі, включаючи різноманітні сенсори, пристрої зв'язку та системи управління, які

співпрацюють між собою та забезпечують різноманітні функції, що дозволяють забезпечити комфорт та безпеку мешканців.

Проведено аналіз обладнання Cisco, яке має деякі переваги порівняно з іншими системами, зокрема, можливість забезпечення високої швидкості передачі даних, надійність та безпеку мережі. Розглянуто особливості використання обладнання Cisco в «розумному» домі, зокрема, можливості інтеграції з іншими системами управління та забезпечення віддаленого керування.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ ПРОДУКТУ CISCO MERAKI MX

3.1 Налаштування мережі та з'єднання обладнання Cisco Meraki

Налаштування мережі та з'єднання обладнання Cisco Meraki - це важлива частина роботи зі створення «розумного» будинку з використанням обладнання Cisco. Для налагодження мережі та з'єднання обладнання Cisco Meraki можна використовувати хмарну платформу Meraki Dashboard. Для цього потрібно зареєструватися на платформі та додати обладнання до списку. Після цього можна налаштувати мережу, встановити параметри безпеки, додати користувачів та відслідковувати активність в мережі.

Однією з переваг обладнання Cisco Meraki є автоматична настройка, яка дозволяє просто підключити пристрої до мережі та забезпечити їх автоматичною настройкою. Крім того, Meraki Dashboard має інтуїтивно зрозумілий інтерфейс, що дозволяє користувачам швидко налаштувати мережу та контролювати її роботу.

На Cisco Meraki існує кілька способів налаштування мережі та з'єднання обладнання. Одним з них є з'єднання з використанням хмарної платформи Meraki Dashboard. Ця платформа дає змогу здійснювати віддалене керування обладнанням, налаштування мережі та моніторинг її стану.

Для підключення до платформи Meraki Dashboard необхідно спочатку створити обліковий запис і зареєструвати обладнання на платформі. Для реєстрації обладнання можна скористатися ключем ліцензії, який зазвичай надається разом з обладнанням. Після реєстрації обладнання в системі можна почати його налаштування через платформу Meraki Dashboard.

Іншим способом налаштування обладнання Cisco Meraki є його локальне з'єднання через консольний порт. Для цього потрібно підключити обладнання до локальної мережі і зайти в консольний режим. Через консольний порт можна

налаштувати базові параметри обладнання, такі як IP-адресу, маску підмережі, шлюз за замовчуванням та інші параметри.

Також, налаштування мережі та з'єднання обладнання Cisco Meraki можна проводити через API. API дає змогу програмно керувати обладнанням та налаштовувати мережу за допомогою програмного коду. Це може бути корисно для автоматизації процесів та інтеграції з іншими системами.

Незалежно від того, який спосіб налаштування буде обраний, обладнання Cisco Meraki пропонує широкі можливості для налаштування мережі та забезпечення її стабільності та безпеки.

При налаштуванні мережі можна використовувати різні типи обладнання Cisco Meraki, такі як точки доступу, комутатори та мережеві контролери. Кожен з цих пристроїв має свої особливості та може бути настроєний відповідно до потреб користувача. Наприклад, точки доступу можна налаштувати для роботи в різних режимах, включаючи мережеву ізоляцію, гостьовий доступ та управління мережею через соціальні мережі.

Після налаштування мережі та з'єднання обладнання Cisco Meraki можна розпочати тестування та аналіз його роботи в "розумному" домі. Для цього можна використовувати різні інструменти, такі як засоби моніторингу трафіку, аналізатори мережі та засоби відслідковування активності користувачів.

Налаштування мережі та з'єднання обладнання Cisco Meraki зазвичай здійснюються за допомогою хмарного сервісу, що дозволяє віддалено керувати та налаштовувати всі пристрої з одного місця.

Для того, щоб підключити обладнання Cisco Meraki до мережі, потрібно встановити відповідні драйвери та програмне забезпечення. Після цього можна приступити до налаштування самої мережі.

Один з основних елементів мережі Cisco Meraki - це шлюз безпеки, який виступає як центральний об'єкт управління мережею. Для налаштування шлюзу безпеки потрібно спочатку встановити його фізично на місці та підключити до мережі. Після цього, використовуючи хмарну панель управління Cisco Meraki, можна створити нову мережу та налаштувати її параметри.

Для налаштування з'єднання обладнання Cisco Meraki між собою та з шлюзом безпеки використовуються різні протоколи та технології, зокрема Wi-Fi, Ethernet, Bluetooth та інші. Для забезпечення максимальної стійкості та надійності з'єднання рекомендується використовувати високоякісні мережеві кабелі та мережеве обладнання.

Загалом, налаштування мережі та з'єднання обладнання Cisco Meraki вимагає досвідченого IT-спеціаліста з глибоким розумінням мережевих протоколів та технологій. Однак, завдяки хмарному сервісу та простому інтерфейсу управління, процес налаштування може бути значно спрощений [11].

Для цього потрібно виконати наступні кроки:

- Підготовка пристроїв до підключення. Забезпечення наявності всіх необхідних деталей, таких як кабелі Ethernet, блоки живлення, монтажні кільця тощо.
- Планування мережі. Для забезпечення оптимальної роботи мережі необхідно ретельно спланувати її архітектуру та розміщення точок доступу, комутаторів та інших пристроїв.
- Налаштування обладнання. Після підключення пристроїв до мережі необхідно налаштувати їх, використовуючи веб-інтерфейс Meraki Dashboard.
- Створення мережі. У Meraki Dashboard створіть нову мережу та додайте до неї всі підключені пристрої.
- Налаштування політик безпеки та мережевих послуг. У Meraki Dashboard налаштуйте правила безпеки та доступу до мережевих послуг для кожного підключеного пристрою.
- Тестування мережі. Перед введенням мережі в експлуатацію необхідно провести тестування мережі, щоб переконатися у її правильному функціонуванні.
- Аналіз результатів тестування. Після завершення тестування необхідно проаналізувати результати, виявити та виправити помилки, якщо вони є, та підготувати мережу до введення в експлуатацію.

3.2 Налаштування безпеки Cisco Meraki MX

Налаштування безпеки в Cisco Meraki є одним з найважливіших етапів при впровадженні «розумного» будинку. Враховуючи, що розумний будинок повинен бути захищеним від несанкціонованого доступу, крадіжки та вторгнень у мережу, необхідно встановити ефективну систему захисту.

Однією з головних функцій безпеки є захист мережі від атак ззовні. Cisco Meraki може відслідковувати небажані підключення до мережі та блокувати їх, що допомагає зменшити ризик компрометації мережі. Для досягнення цієї мети використовується інтелектуальна система захисту, яка аналізує дані з пристроїв та визначає, які з них мають доступ до мережі.

Крім того, необхідно налаштувати захист від внутрішніх загроз, зокрема, від зловмисників, які можуть спробувати вторгнутися в систему з приводу відсутності необхідного захисту. Для цього використовується різноманітні методи, такі як шифрування трафіку, автентифікація користувачів та мережевий доступ контролера.

Окрім захисту від зовнішніх та внутрішніх загроз, необхідно також забезпечити фізичну безпеку пристроїв. Це може бути досягнуто за допомогою контролю доступу до серверних кімнат, монтажу відеокамер та використання системи виявлення інцидентів.

Зазвичай адміністратори невеликих та середніх компаній часто не використовують більшість функцій свого корпоративного фаєрволу. За статистикою основних причин цього кілька. У 25 % випадків головні налаштування виконані, але в інші адміністратора бракує часу. Ще в 34% випадків вони не впоралися з налаштуваннями. І в 41% випадків всі наявні функції просто не потрібні їм. З цього можна дійти невтішного висновку: шлюз безпеки потрібно вибирати лише відповідно до власних завдань, потреб і можливостей, не орієнтуючись на весь перелік функцій [12].

Для вимог більшості компаній - як малих і середніх, так і великих з географічно розподіленою інфраструктурою - чудово підійдуть шлюзи безпеки

Cisco Meraki MX. Вони прості в налаштуванні, не вимагають присутності адміністраторів безпеки у віддалених філіях і водночас використовують ті ж самі набори сигнатур.

Перший етап налаштування:

1. Вибрати режим роботи VPN-концентратора (у центрі вибрано режим Hub, так що натискаємо Spoke).

2. Для Spoke вибрати режим тунелювання Split, щоб використовувати VPN-тунель тільки для трафіку до центрального офісу, а інтернет-трафік випускати безпосередньо «світло».

3. Усі підмережі вже підраховані, необхідно лише вибрати, які можуть використовувати VPN (вказати напроти yes/no).

4. Збереження. Тепер хмара Meraki сама погодить адресацію та параметри тунелів IPsec AES128 та поширить дані про VPN-маршрути на пристрої MX у мережі (рис. 3.1).

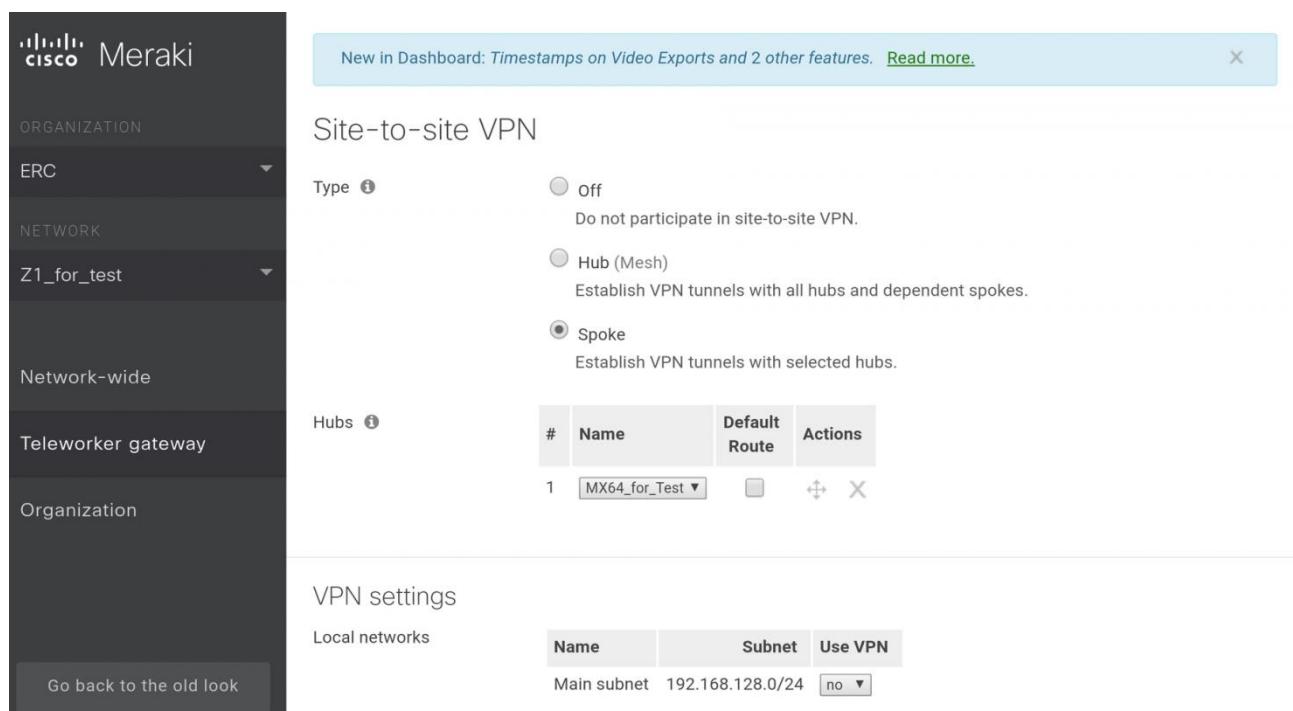


Рис.3.1. Процес автоматичної адресації та налаштування тунелів

Другий етап:

1. Увімкнути антивірусне сканування (Malware prevention – enabled).

2. Увімкнути захист від несанкціонованого доступу на базі SourceFire (Intrusion detection and prevention – вибрати Mode Prevention).

3. Вибрати із трьох встановлених наборів правил IPS від найбільш лояльного до рестриктивного (Connectivity/Balanced/Security).

4. Зберегти. Тепер система захищена та можливо переглядати аналітику (рис. 3.2).

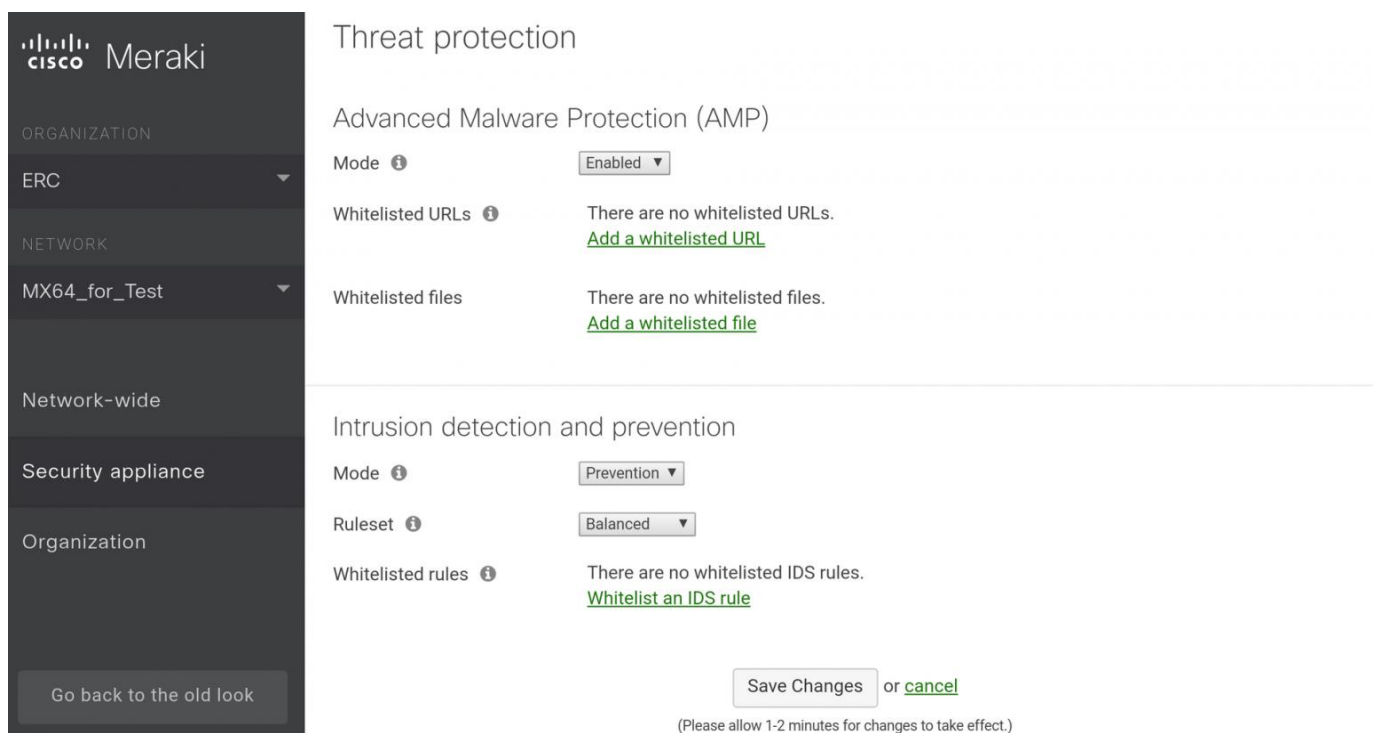


Рис.3.2. Налаштування захисту від несанкціонованого доступу та вірусів в Cisco Meraki

Допустиме використання інтернету. Система фільтрації контенту забезпечує безпечне використання інтернету, користувачами всередині мережі. Коли користувач запитує якусь URL-адресу, він перевіряється в кілька етапів і може бути заблокований до перегляду через наявність шкідливого або небажаного контенту.

Етап налаштування:

1. Вибір категорії web-сайтів, які необхідно заблокувати (рекомендуємо блокувати Adult, Bot Nets, Confirmed SPAM Sources, Illegal, Malware Sites, Phishing, Proxy Avoidance, SPAM URLs, Spyware).

2. Увімкнути фільтрацію пошукових запитів (Web search filtering – enabled).
3. Увімкнути фільтрацію YouTube (YouTube for schools – enabled).
4. Зберегти. Тепер у співробітників компанії або студентів обмежений доступ до сайтів, які не можна використовувати на робочому місці (рис.3.3).

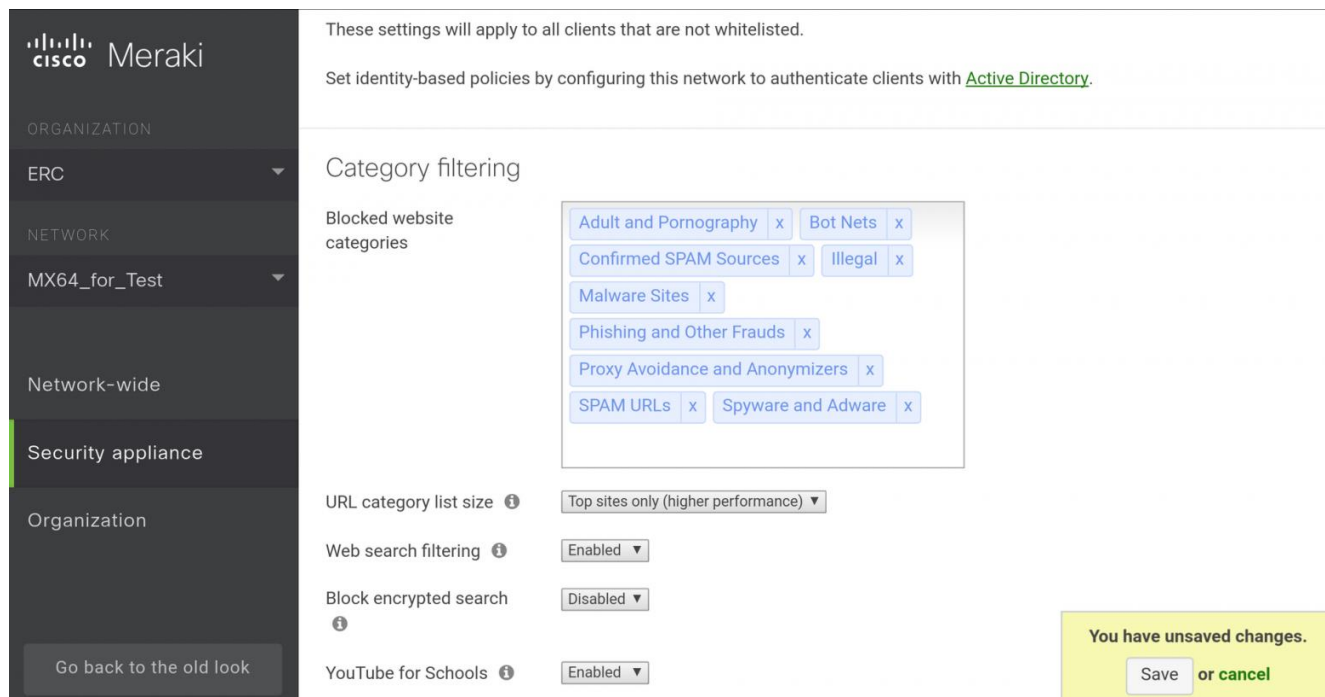


Рис.3.3. Обмеження доступу до web-сайтів за допомогою фільтрації та блокування категорій

Шейпінг та пріоритезація трафіку. Разом із планомірним збільшенням швидкостей передачі у телекомунікаціях збільшується частка інтерактивного трафіку, вкрай чутливого до параметрів середовища транспортування. Тому завдання забезпечення якості обслуговування (Quality of Service - QoS) стає все більш актуальною. Необхідно, щоб бізнес-критичні програми мали пріоритет над різними мультимедійними і не страждали від заповнення каналу.

Етап налаштування:

1. Вибір параметрів допустимого завантаження вхідного та вихідного трафіку для обох WAN-аплінків (також є можливість підключити 3G/4G-модем як додатковий аплінк для забезпечення стійкості до відмови).
2. Включити вирівнювач навантаження між аплінками (Load Balancing – enabled).

3. Увімкнути правила шейпінгу трафіку. Для VoIP і Videoconferencing встановити пріоритет High. Для категорій Peer-to-peer, Online backup, Video & Music виставити обмеження по смузі пропускання та пріоритет Low.

4. З такими налаштуваннями навіть у разі обмеженої пропускної спроможності каналу користувачі не помітять зниження швидкості передачі даних: канал для бізнес-додатків не засмічуватиметься вихідним трафіком. Ці функції доступні на всіх шлюзах безпеки Cisco Meraki MX, залишилося лише вибрати необхідну модель залежно від ваших потреб, наявності WiFi, PoE, специфічних портів (рис. 3.4, 3.5).

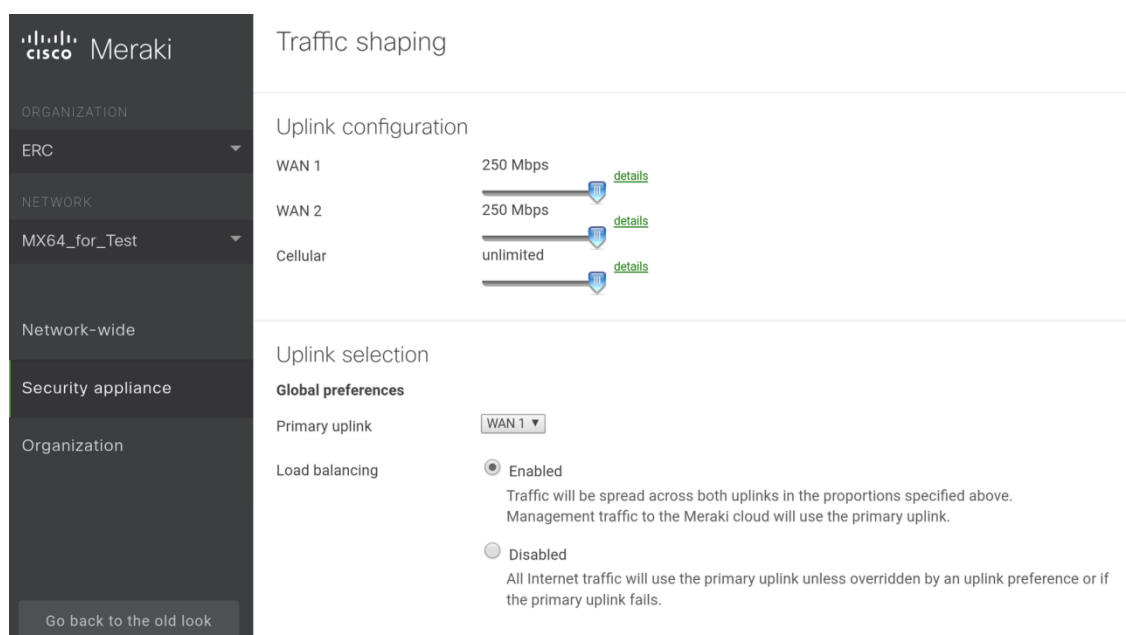


Рис.3.4. Налаштування параметрів для оптимізації роботи мережі з використанням шлюзів безпеки Cisco Meraki MX

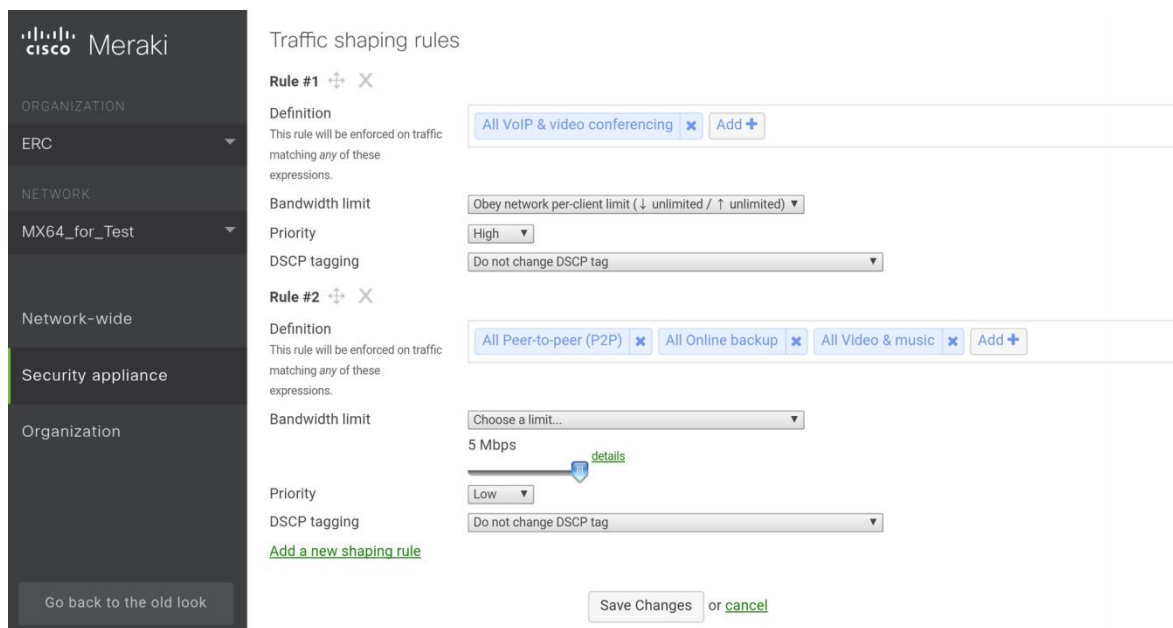


Рис.3.5. Налаштування шлюза безпеки Cisco Meraki MX для оптимального управління трафіком

3.3 Рекомендації щодо підвищення ефективності використання обладнання Cisco Meraki MX

Налаштування правил безпеки є однією з найважливіших частин ефективного використання обладнання Cisco Meraki MX. Правила безпеки допомагають захистити вашу мережу від зловмисників, захистити дані та забезпечити безпеку мережі. Для досягнення максимальної ефективності використання обладнання Cisco Meraki MX варто налаштувати наступні правила безпеки:

- **Firewall:** Налаштовувати брандмауер для блокування небажаного трафіку. Встановіть правила, які обмежують доступ до мережі, включаючи заборону доступу до певних портів та протоколів.
- **Content Filtering:** Застосовувати фільтрацію контенту для блокування доступу до небажаного контенту в мережі, такого як сайти зі шкідливим програмним забезпеченням або соціальні мережі.

- Intrusion Prevention: Використання системи запобігання вторгненням (IPS), щоб захистити мережу від атак зловмисників.

Регулярне оновлення програмного забезпечення. Cisco Meraki зазвичай випускає оновлення програмного забезпечення з різними фіксами та покращеннями функцій. Необхідно моніторити оновлення регулярно та встановлювати їх, щоб забезпечити максимальну ефективність та безпеку мережі.

Налаштування правил мережі. Cisco Meraki MX дозволяє налаштовувати різні правила мережі, такі як правила доступу, правила переадресації та правила маршрутизації.

Налаштування правил QoS. Cisco Meraki MX дозволяє налаштовувати правила QoS (Quality of Service), щоб забезпечити пріоритетний доступ до ресурсів для різних типів трафіку. Слід налаштовувати ці правила, щоб забезпечити ефективне використання доступної пропускної здатності мережі.

Застосовування додаткових функцій. Cisco Meraki MX має багато додаткових функцій, таких як виявлення загроз, захист від вторгнень, заборона доступу до сайтів та багато іншого. Слід використовувати ці функції, щоб забезпечити максимальний захист та ефективність мережі.

Налаштування мережевих пристроїв. Щоб забезпечити максимальну ефективність мережі, необхідно налаштовувати всі мережеві пристрої, такі як комутатори, маршрутизатори та точки доступу до Wi-Fi.

Висновки до третього розділу

Досліджено основні етапи налаштування мережі та з'єднання обладнання Cisco Meraki MX, включаючи встановлення з'єднання з Інтернетом, створення мережі, налаштування функцій безпеки та додавання пристроїв до мережі. Розглянуто різні варіанти налаштування безпеки, включаючи налаштування VPN, вирівнювача навантаження та шейпінгу трафіку.

Проаналізовано використання хмарних сервісів для зберігання налаштувань та моніторингу стану мережі, налаштування правильної схеми мережі та

оптимізацію налаштувань для забезпечення оптимальної швидкості передачі даних.

Розроблено рекомендації, для підвищення ефективності використання обладнання Cisco Meraki MX, які можуть допомогти забезпечити оптимальну роботу мережі та забезпечити надійний та безпечний доступ до Інтернету для користувачів.

ВИСНОВКИ

В бакалаврській роботі отримано наступні наукові та науково-практичні результати:

- досліджено характеристики обладнання Cisco для створення розумного будинку, визначено особливості його використання та налагодження мережі;
- досліджено технології, що використовуються в розумному домі, законодавче регулювання в галузі розумних будинків, обладнання Cisco та його особливості;
- проаналізовано можливості обладнання Cisco для створення розумного дому та вибір обладнання, технологій для його створення;
- проведений аналіз налаштування мережі та з'єднання обладнання Cisco Meraki MX, налаштування безпеки Cisco Meraki та рекомендації щодо підвищення ефективності використання обладнання Cisco Meraki MX;
- реалізовано налаштування параметрів для оптимізації роботи мережі з використанням шлюзів безпеки, налаштування захисту від несанкціонованного доступу та захист від вірусів, а також процес автоматичної адресації та налаштування тунелів.

Отже, вирішення завдання зі створення розумного будинку з використанням обладнання Cisco потребує компетентного аналізу та вибору відповідного обладнання, а також налагодження мережі та забезпечення її безпеки. «Розумний» будинок на основі технології Cisco може бути ефективним та зручним рішенням для забезпечення комфортного та безпечного життя.