Міністерство освіти і науки України
Криворізький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерних систем та мереж

Пояснювальна записка
до кваліфікаційної роботи бакалавра
за спеціальністю 123 «Комп'ютерна інженерія»

на тему: ПРОЕКТУВАННЯ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ РОЗУМНОГО ДОМУ

Проектував _____ Р. С. Шапран

Керівник роботи _____ А. О. Сенько

Нормоконтроль _____ Д. І. Кузнєцов

Завідувач кафедри _____ А. І. Купін

Кривий Ріг
2025

Криворізький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерних систем та мереж

Ступінь вищої освіти бакалавр
Спеціальність 123 «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач кафедри, голова циклової комісії

_____ А. І. Купін

"____" _____ 20__ року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

_____
(прізвище, ім'я, по батькові)

1. Тема роботи _____
_____
_____

керівник роботи _____,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від "___"_____ 20__року №__

2. Строк подання студентом роботи _____

3. Вихідні дані до роботи _____
_____
_____
_____
_____
_____

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)_____
_____
_____
_____
_____
_____

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)_____
_____
_____
_____
_____

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Строк виконання етапів роботи	Примітка

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник роботи _____ _____
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 75 сторінок, 3 рисунки, 21 використаних джерел.

У бакалаврській роботі проведено комплексне дослідження процесу розробки, реалізації та впровадження інтелектуальної системи для управління функціями «розумного дому» з підвищеним рівнем безпеки. Проєкт передбачає створення модульної цифрової інфраструктури, що поєднує IoT-пристрої, систему відеоспостереження, мережевий сервер з аналізом трафіку та автоматизованими сценаріями реагування на події.

У першому розділі обґрунтовано актуальність роботи, вивчено стан сучасних рішень у галузі «розумного дому» та проведено аналіз відповідних технологій — від IoT-протоколів (MQTT, Zigbee, Z-Wave) до архітектури управління в локальних мережах. Розглянуто вимоги до безпеки таких систем та описано типові загрози, що виникають у пов’язаному середовищі.

У другому розділі деталізовано процес побудови інфраструктури: обрана апаратна база, реалізована серверна платформа на базі Ubuntu Server, інтегровано систему моніторингу трафіку Suricata, IoT-шлюзи, IP-камери з підтримкою ONVIF/RTSP. Проведено первинне конфігурування міжмережевого екрану, SSH-доступу та резервного копіювання.

У третьому розділі описано методики централізованого управління системою через Home Assistant та сценарії автоматизації. Налаштовано логіку реагування на мережеві події, API-інтеграцію, обробку логів через Grafana і Kibana. Здійснено розширення функціоналу за рахунок можливості підключення сторонніх сервісів через MQTT та REST.

У четвертому розділі проведено функціональні, безпекові та стрес-тести. Виявлено здатність системи ефективно обробляти до 10 000 пакетів на секунду із середнім часом спрацювання 2–3 секунди. У логах зафіксовано точність виявлення понад 98 % атак типу DoS, сканування портів та аномального DNS-трафіку. Проведено аналіз зручності експлуатації через веб-інтерфейс, мобільний застосунок та SSH-консоль.

У п’ятому розділі розроблено план подальшого розвитку: інтеграція із SIEM-платформами, впровадження алгоритмів машинного навчання, розширення можливостей за рахунок edge computing та створення комерційної моделі з поділом на модулі. Розглянуто маркетингові стратегії просування продукту, можливості укладення партнерських угод з виробниками обладнання та провайдерами послуг.

Ключові слова: РОЗУМНИЙ ДІМ, IOT, SURICATA, MQTT, ONVIF, АВТОМАТИЗАЦІЯ, ДОМАШНЯ МЕРЕЖА, КІБЕРБЕЗПЕКА, SSH, API, ВІДЕОСПОСТЕРЕЖЕННЯ, IDS, HOME ASSISTANT, GRAFANA, ПРОТОКОЛИ ЗВ’ЯЗКУ.

Explanatory note: 75 pages, 3 figures, 21 sources used. The bachelor's thesis presents a comprehensive study of the development, implementation, and deployment of an intelligent system for managing smart home functions with an enhanced level of security. The project involves the creation of a modular digital infrastructure combining IoT devices, a video surveillance system, a network traffic analysis server, and automated response scenarios.

Chapter one substantiates the relevance of the study, examines the current state of smart home technologies, and analyzes relevant protocols—from MQTT, Zigbee, and Z-Wave to local network control architectures. Security requirements and typical threats in connected environments are also outlined.

Chapter two details the infrastructure design: the hardware platform selection, deployment of a server based on Ubuntu Server, integration of the Suricata traffic monitoring system, IoT gateways, and IP cameras supporting ONVIF and RTSP. Initial configurations of the firewall, SSH access, and backup procedures are completed.

Chapter three focuses on centralized system management using Home Assistant and describes automation scenarios. Response logic to network events is defined, API integration and log processing through Grafana and Kibana are configured. Functionality is extended through the integration of third-party services via MQTT and REST protocols.

Chapter four covers functional, security, and stress testing. The system demonstrated the ability to handle up to 10,000 packets per second with an average response time of 2–3 seconds. Logs confirmed over 98% detection accuracy for DoS attacks, port scanning, and anomalous DNS traffic. Usability was assessed through the web interface, mobile application, and SSH console.

Chapter five outlines the development roadmap: integration with SIEM platforms, implementation of machine learning algorithms, expansion via edge computing, and a modular commercial model. Marketing strategies are discussed, along with partnership opportunities with hardware vendors and service providers.

Keywords: SMART HOME, IOT, SURICATA, MQTT, ONVIF, AUTOMATION, HOME NETWORK, CYBERSECURITY, SSH, API, VIDEO SURVEILLANCE, IDS, HOME ASSISTANT, GRAFANA, COMMUNICATION PROTOCOLS.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

- РД – розумний дім;
- ОС – операційна система;
- IoT – Internet of Things (Інтернет речей);
- LAN – Local Area Network (локальна обчислювальна мережа);
- WAN – Wide Area Network (глобальна мережа);
- IP – Internet Protocol (інтернет-протокол);
- MAC – Media Access Control (адреса фізичного рівня мережі);
- SSH – Secure Shell (захищене мережеве з’єднання);
- UFW – Uncomplicated Firewall (спрощений міжмережевий екран);
- IDS – Intrusion Detection System (система виявлення вторгнень);
- IPS – Intrusion Prevention System (система запобігання вторгнень);
- SIEM – Security Information and Event Management (керування інформацією та подіями безпеки);
- API – Application Programming Interface (інтерфейс прикладного програмування);
- JSON – JavaScript Object Notation (текстовий формат зберігання даних);
- TCP – Transmission Control Protocol (протокол управління передачею);
- UDP – User Datagram Protocol (протокол пакетної передачі даних);
- RTSP – Real Time Streaming Protocol (протокол потокової трансляції);
- ONVIF – Open Network Video Interface Forum (мережевий відеоінтерфейс);
- MQTT – Message Queuing Telemetry Transport (протокол телеметрії на основі черги повідомлень);
- TLS/SSL – Transport Layer Security / Secure Sockets Layer (протоколи захисту транспортного рівня);
- VPN – Virtual Private Network (віртуальна приватна мережа);
- DoS – Denial of Service (атака на відмову в обслуговуванні);
- DNS – Domain Name System (система доменних імен);
- GUI – Graphical User Interface (графічний інтерфейс користувача);
- CLI – Command Line Interface (інтерфейс командного рядка);
- CPU – Central Processing Unit (центральний процесор);
- RAM – Random Access Memory (оперативна пам’ять);
- HDD – Hard Disk Drive (жорсткий диск);
- SSD – Solid-State Drive (твердотільний накопичувач).

ВСТУП

У сучасних умовах стрімкого розвитку цифрових технологій та широкого впровадження концепції «Інтернету речей» важливість створення інтелектуальних систем управління житлом набуває особливого значення. Розумний дім, як комплекс систем, що інтегрують IoT-пристрої, IP-камери, датчики, смарт-розетки та інше обладнання, дозволяє не лише забезпечити автоматизацію побутових процесів, а й підвищити рівень безпеки, енергоефективності та комфорту для мешканців. Ця дипломна робота присвячена розробці та дослідженню системи інтелектуального управління «розумним домом», яка об’єднує сучасні методи моніторингу мережевого трафіку, аналізу подій та управління IoT-компонентами.

Метою даної роботи є концептуалізація та впровадження інтегрованого рішення для забезпечення централізованого контролю над різноманітними пристроями в межах локальної мережі, створення умов для оперативного реагування на кібератаки та оптимізації енергоспоживання. Для досягнення цієї мети було проведено глибокий аналіз сучасних протоколів зв’язку (Ethernet, Wi-Fi, RTSP, ONVIF, MQTT, Zigbee, Z-Wave) та засобів забезпечення кібербезпеки, зокрема використання IDS/IPS систем як Suricata. Теоретичний аналіз доповнюється експериментальним тестуванням розробленої системи в умовах лабораторного середовища та пілотного впровадження, що дозволяє визначити її продуктивність, точність виявлення загроз та адаптивність до змін умов мережевої експлуатації.

У роботі обговорено не тільки технічні аспекти реалізації системи, але і розглянуто питання інтеграції з хмарними сервісами, SIEM-платформами та аналітичними інструментами, що сприятимуть централізованій обробці даних і забезпеченню високого рівня безпеки. Важливим компонентом дослідження стала оцінка можливостей масштабування системи та її адаптації під різні сегменти ринку – від приватного житла до комерційних об’єктів.

Отримані результати демонструють, що запропоноване рішення є конкурентоспроможним за рахунок високої продуктивності, надійності та здатності адаптуватися до зростаючого навантаження мережі. Розроблене комплексне рішення сприятиме підвищенню рівня комфорту, безпеки та енергоефективності сучасного житлового простору, що є надзвичайно актуальним в епоху цифрової трансформації. Це дослідження створює основу для подальших розробок у сфері автоматизації «розумного дому» та впровадження інноваційних технологій як у приватному, так і в комерційному секторах.

1 АНАЛІТИЧНИЙ ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Коротко про концепцію «розумного дому»

У сучасному світі, що характеризується стрімким розвитком інформаційних технологій, електроніки та телекомунікацій, поняття «розумного дому» (smart home) набуває дедалі більшого значення у житті людини. Якщо ще кілька десятків років тому автоматизовані системи керування побутом здавалися елементом наукової фантастики, то сьогодні вони стають доступними для широкого кола користувачів і поступово інтегруються в повсякденне життя.
Розумний дім – це сукупність апаратних і програмних рішень, спрямованих на забезпечення максимальної зручності, безпеки, енергоефективності, а також оптимізації побутових процесів і ресурсів у житлових приміщеннях.

Сутність і головна ідея концепції:

Основою концепції розумного дому є створення цілісної екосистеми, де всі пристрої, системи й електроніка житла взаємодіють між собою. Ключовою ідеєю є централізоване або розподілене керування всіма підсистемами будинку — такими як освітлення, клімат-контроль, системи безпеки, побутова техніка, мультимедіа, доступ і багато інших — через єдиний зручний інтерфейс.

Це дає змогу власнику будинку не лише здійснювати ручне керування різними приладами, а й задавати певні сценарії чи алгоритми дій, які виконуються автоматично, виходячи з визначених умов або подій. Наприклад, автоматичне ввімкнення освітлення при появі людини у кімнаті, зміна температурного режиму вночі, вимкнення всіх електроприладів у разі відсутності мешканців, блокування дверей тощо.

Основні компоненти та пристрої розумного дому:

До основних складових розумного дому можна віднести велику кількість пристроїв, серед яких:

- **Системи освітлення** (інтелектуальні лампи, димери, сенсори присутності);
- **Системи безпеки** (відеокамери, сигналізації, електронні замки, датчики диму, руху, протікання води, сенсори відчинення дверей і вікон);
- **Побутова техніка** (інтелектуальні холодильники, пральні та посудомийні машини, кавомашини, кухонна техніка із підключенням до мережі);
- **Мультимедійні пристрої** (телевізори, аудіосистеми, домашні кінотеатри, smart speakers);
- **Мережеве обладнання** (Wi-Fi-роутери, хаби, мережеві накопичувачі).

Кожен із цих пристроїв може функціонувати окремо, однак головна цінність розумного дому полягає у їхній взаємодії й інтеграції в єдину систему.

Принципи керування та взаємодії пристроїв:

Взаємодія пристроїв у розумному домі може відбуватися за допомогою різних моделей керування:

- **Централізоване керування** — усі пристрої підключаються до центрального контролера (хаба), який координує їхню роботу й надає інтерфейс для користувача;
- **Децентралізоване (розподілене) керування** — окремі пристрої спілкуються напряму, обмінюючись даними та командами через локальну мережу або Інтернет;
- **Хмарні сервіси** — частина функціоналу й зберігання даних виноситься на зовнішні сервери, що дає змогу керувати будинком з будь-якої точки світу;
- **Гібридні рішення** — поєднують переваги локального й віддаленого керування, забезпечуючи більшу гнучкість та надійність системи.

Для зручності користувача розробляються мобільні додатки, веб-інтерфейси, голосові асистенти, настінні панелі керування, які дозволяють здійснювати моніторинг і керування як окремими пристроями, так і цілими сценаріями дій.

Інтеграція та побудова екосистеми:

Одним із головних завдань при створенні розумного дому є інтеграція різних пристроїв, які можуть використовувати різні протоколи зв’язку та мати різних виробників. Для цього застосовуються такі сучасні технології, як Internet of Things (IoT), які дозволяють об’єднувати найрізноманітніші пристрої в одну розподілену мережу. IoT-екосистема забезпечує обмін даними, зворотний зв’язок, а також можливість централізованої або розподіленої обробки інформації.

Інтеграція сприяє підвищенню гнучкості у налаштуванні системи, створенню багаторівневих сценаріїв та ефективному управлінню всіма побутовими процесами. Зокрема, це дає змогу побудувати такі сценарії, як автоматичне вмикання освітлення лише в тих приміщеннях, де є люди, регулювання температури у різних зонах будинку, або сповіщення власника у разі виявлення незвичної активності.

Безпека та надійність системи:

Забезпечення безпеки мешканців і майна — один із найпріоритетніших напрямів розвитку розумного дому. Сучасні інтелектуальні системи дозволяють не лише сповіщати власника про підозрілі ситуації (проникнення, пожежу, протікання води), а й автоматично реагувати на них — наприклад, перекривати подачу води або електроенергії, запускати сценарій евакуації, автоматично викликати аварійні служби чи надсилати сповіщення відповідальним особам через Інтернет.

Варто також зазначити, що захист даних і приватності у розумному домі стає все більш актуальним, адже велика кількість пристроїв підключені до Інтернету, обробляють і зберігають особисту інформацію.

Енергоефективність і раціональне використання ресурсів:

Однією з головних переваг розумного дому є можливість суттєвого підвищення енергоефективності житла та забезпечення оптимального використання всіх доступних ресурсів. Завдяки застосуванню інтелектуальних алгоритмів, сучасні системи автоматизації здатні самостійно визначати режими роботи електрообладнання, керувати освітленням, опаленням, кондиціонуванням повітря, а також оптимізувати споживання води, газу та інших енергоносіїв. Наприклад, система може автоматично вимикати освітлення чи електроприлади у тих приміщеннях, де протягом певного часу не фіксується рух або присутність людини. Кліматичне обладнання (обігрівачі, кондиціонери, вентилятори) може підлаштовувати свою роботу відповідно до поточних погодних умов, часу доби, індивідуальних побажань мешканців або навіть динамічно змінювати режими з урахуванням тарифів на електроенергію, з метою економії коштів. Крім того, такі системи можуть контролювати рівень вологості, якість повітря, температуру та автоматично відкривати чи закривати вікна для провітрювання. Завдяки подібному підходу вдається не лише зменшити загальне енергоспоживання, а й оптимізувати комунальні витрати, підвищити комфорт перебування в оселі та зробити вклад у захист довкілля через зменшення викидів CO_2 та інших забруднювальних речовин. Деякі системи навіть дозволяють відслідковувати історію споживання ресурсів, створювати звіти та аналізувати динаміку, що допомагає виявляти нераціональні витрати і вчасно реагувати на аварійні ситуації (наприклад, протікання води чи перевантаження мережі).

Сучасні тенденції розвитку розумного дому нерозривно пов’язані з інтеграцією новітніх досягнень у сфері штучного інтелекту, машинного навчання, хмарних обчислень та широкого використання мобільних пристроїв і додатків. Це відкриває нові горизонти для персоналізації систем, дозволяє реалізувати адаптивні сценарії керування, що враховують індивідуальні звички, поведінку та розклад мешканців. Дедалі більше розумних систем здатні самостійно аналізувати великі об’єми даних від сенсорів і пристроїв, прогнозувати майбутні події (наприклад, зміни клімату в оселі, попит на енергію), а також автоматично виявляти й попереджати про можливі проблеми або небезпечні ситуації. Використання хмарних технологій забезпечує зручний віддалений доступ до керування системою з будь-якої точки світу, дає змогу оновлювати програмне забезпечення, впроваджувати нові функції й зберігати важливі дані в безпечному середовищі.

Отже, концепція розумного дому є надзвичайно актуальною для сучасного суспільства, оскільки поєднує в собі інновації, автоматизацію, індивідуальний підхід до організації побуту й турботу про безпеку та комфорт людини. Інтенсивний розвиток технологій робить розумний дім дедалі доступнішим для масового користувача, перетворюючи мрію про ідеальне житло на реальність сьогодення.

Таким чином, розумний дім стає не лише технологічною інновацією, а й важливою складовою сучасного стилю життя.

1.2 Огляд існуючих рішень

Розвиток концепції розумного дому став можливим завдяки комплексному впровадженню новітніх систем, технологій і протоколів, які забезпечують ефективну взаємодію, просту інтеграцію та високу масштабованість розумних рішень для побуту. За останні десятиліття ринок розумних систем для дому суттєво розширився, пропонуючи безліч як комерційних, так і відкритих платформ. Кожна з них має власні переваги, рівень сумісності, відкритість, особливості інтеграції та рівень підтримки. Завдяки цьому користувачі можуть обирати рішення, які максимально відповідають їхнім потребам, бюджету та існуючій інфраструктурі житла.

Системи автоматизації: типи, архітектури та сучасні підходи:

Усі сучасні системи автоматизації в межах концепції smart home можна умовно поділити на дві основні категорії — централізовані та децентралізовані.

Централізовані системи:

У централізованих системах усі пристрої підключаються до головного контролера або центрального хаба, який виконує функції мозку екосистеми. Саме через цей контролер відбувається координація дій пристроїв, збір і зберігання даних, виконання сценаріїв, а також організація користувацького інтерфейсу для керування всіма підсистемами. Прикладами таких рішень є:

- **Samsung SmartThings** — одна з найпопулярніших комерційних екосистем, що підтримує інтеграцію пристроїв різних виробників та працює з багатьма протоколами зв’язку;
- **Home Assistant** — відкритий програмний продукт з потужною спільнотою, який дозволяє налаштовувати сотні пристроїв, інтегрувати їх у складні сценарії та забезпечує високу гнучкість;
- **Apple HomeKit** — платформа для інтеграції smart-пристроїв від Apple з акцентом на безпеку, простоту налаштування та управління з iOS-пристроїв;
- **Google Home** — екосистема, що орієнтована на простоту, хмарні сервіси та широкий вибір сумісних пристроїв.

Завдяки централізованому підходу користувач отримує єдиний інтерфейс керування усіма системами дому, а взаємодія між пристроями спрощується навіть за наявності різних виробників. Це дозволяє швидко масштабувати систему та додавати нові компоненти без складної інтеграції.

Децентралізовані системи:

Децентралізовані системи (peer-to-peer або mesh-мережі) ґрунтуються на моделі, за якої кожен пристрій здатен напряму спілкуватися з іншими без обов’язкового проходження сигналу через центральний вузол. Завдяки такій архітектурі підвищується надійність (відсутність єдиної точки відмови), розширюються можливості мережі та знижується затримка передачі даних. Яскраві приклади таких систем — рішення на базі протоколів Z-Wave та Zigbee, а також частина рішень на основі MQTT.

Децентралізований підхід дозволяє гнучко адаптувати систему до змін у складі пристроїв, легко розширювати покриття, організовувати багаторівневу передачу даних у великих будинках чи офісах.

Основні технології та стандарти зв’язку:

Ефективність роботи розумного дому напряму залежить від обраних технологій зв’язку, які визначають швидкість, стабільність, енергоспоживання та масштабованість всієї екосистеми.

1. **Wi-Fi (IEEE 802.11)** — найпоширеніший стандарт бездротової передачі даних у розумних будинках. Завдяки високій пропускній здатності та широкому розповсюдженню бездротових маршрутизаторів у житлі Wi-Fi використовується для підключення великих пристроїв — таких як камери відеоспостереження, телевізори, сенсори, розетки, побутова техніка тощо. Основними перевагами є простота налаштування, швидкість передачі даних, масштабованість, підтримка стандартних мережевих протоколів TCP/IP. Однак недоліками залишаються високе енергоспоживання (що не підходить для автономних сенсорів на батарейках) та потенційна перевантаженість частотного діапазону, що може призвести до втрат зв’язку в багатоквартирних будинках.

2. **Zigbee** — один із найпопулярніших енергоефективних протоколів для організації мереж IoT та автоматизації. Протокол побудований на принципах «mesh-мережі», де пристрої не лише отримують сигнали від контролера, а й ретранслюють їх далі, збільшуючи зону покриття та надійність. Zigbee відзначається низьким енергоспоживанням, що ідеально підходить для автономних датчиків руху, температури, вологості, смарт-розеток, освітлення (Philips Hue, Xiaomi Aqara). Підтримка тисяч пристроїв у мережі, швидке підключення нових елементів та висока сумісність роблять Zigbee ідеальним вибором для масштабних інсталяцій.

3. **Z-Wave** — конкурент Zigbee, також побудований на принципі mesh-мереж. Він працює на іншій частоті, що дозволяє уникати перешкод з Wi-Fi, та має ще нижче енергоспоживання. Z-Wave підтримує велику кількість сертифікованих пристроїв різних виробників, проте часто вимагає використання спеціального хаба. Завдяки великому досвіду використання у комерційних і приватних інсталяціях, Z-Wave вважається надійним і стабільним вибором для smart home.

4. **Bluetooth та Bluetooth Low Energy (BLE)** Bluetooth і BLE використовуються для підключення невеликих пристроїв — сенсорів, трекерів, пультів, а також для комунікації з мобільними телефонами. BLE особливо цінується за вкрай мале енергоспоживання, що дозволяє автономно працювати сенсорам до кількох років. Недоліком є обмежена дальність (до 10-20 метрів) і чутливість до перешкод, але для ряду застосувань — наприклад, у квартирах чи кімнатах — Bluetooth є ідеальним.

5. **Ethernet (LAN)** Для пристроїв, де важливі стабільність і швидкість (IP-камери, сервери, телевізори, NAS), використовується класичний дротовий зв’язок Ethernet. Провідне підключення гарантує мінімальні затримки, високу пропускну здатність і захист від радіоперешкод. Водночас Ethernet не підходить для автономних чи часто переміщуваних пристроїв через необхідність прокладання кабелів.

6. **ONVIF (Open Network Video Interface Forum)** — міжнародний стандарт, розроблений для інтеграції та взаємодії IP-відеокамер, відеореєстраторів, контролерів безпеки тощо. Завдяки ONVIF забезпечується сумісність пристроїв різних виробників, стандартизується процес налаштування, управління та архівування відео, що критично важливо для систем безпеки й відеоспостереження.

7. **MQTT (Message Queuing Telemetry Transport)** — легковаговий, надзвичайно ефективний протокол обміну повідомленнями, що спеціально розроблений для IoT, автоматизації та телеметрії. Він дозволяє організувати надійний і захищений обмін даними між різними пристроями, серверами, додатками навіть у нестабільних мережах. Протокол підтримує ієрархічну структуру тем (topics), гнучке налаштування прав доступу, шифрування і легко масштабується для великих мереж.

8. **Thread** — відносно новий протокол для IoT, розроблений з урахуванням високої безпеки, самовідновлення мережі та простоти налаштування. Підтримується багатьма сучасними системами (наприклад, Google Nest, Apple HomePod) і є частиною відкритого стандарту Matter, який має на меті забезпечити уніфіковану сумісність пристроїв у майбутньому.

Програмне забезпечення для автоматизації та сценаріїв:

Управління та автоматизація розумного дому відбувається завдяки спеціалізованим програмним платформам, які забезпечують інтеграцію пристроїв, організацію сценаріїв та зручне керування для користувача.

1. **Home Assistant** — потужна відкрита платформа, яку можна розгорнути на сервері, міні-ПК або одноплатних комп’ютерах (наприклад, Raspberry Pi). Вона підтримує інтеграцію сотень пристроїв, дозволяє створювати складні сценарії, автоматизацію за тригерами (датчиками, подіями), має підтримку основних протоколів, велику бібліотеку модулів і розширень, активну спільноту та регулярні оновлення.

2. **OpenHAB** – Ще одна популярна open-source платформа для організації розумного дому. Відзначається високою гнучкістю, підтримкою практично всіх стандартів та пристроїв, масштабованістю, можливістю роботи як з локальною, так і з хмарною автоматизацією.

3. **Domoticz, ioBroker, MajorDomo** – Ці платформи також належать до відкритих рішень і забезпечують багатий функціонал — гнучке налаштування сценаріїв, підтримку численних плагінів та драйверів, веб-інтерфейси та API для інтеграції з іншими системами.

4. **Програмні рішення виробників**. Багато відомих брендів створюють власні програмні платформи (Xiaomi Mi Home, Samsung SmartThings, Google Home, Amazon Alexa), які зручні для користувача, але часто працюють лише з обладнанням певного виробника чи екосистеми або мають обмежену інтеграцію з пристроями сторонніх компаній. Основною перевагою таких рішень є простота налаштування й використання, інтуїтивний інтерфейс, але мінусом — залежність від хмарних сервісів і закритість протоколів.

Методи автоматизації: локальна, хмарна та гібридна:

Розумний дім дозволяє організовувати сценарії автоматизації, які можуть виконуватися у різних режимах:

- **Локальна автоматизація** — сценарії обробляються безпосередньо на контролері чи сервері користувача. Такі системи працюють навіть за відсутності доступу до Інтернету, що підвищує їхню надійність, безпеку та приватність. Наприклад, при спрацюванні датчика руху одразу локально вмикається світло або запускається тривога;

- **Хмарна автоматизація** — основна логіка й зберігання даних винесені на сервери виробника або в хмарні сервіси. Це дозволяє віддалено керувати системою, отримувати сповіщення, оновлювати ПЗ, інтегрувати нові функції, але може створювати залежність від стабільності Інтернету і серверів;

- **Гібридна автоматизація** — поєднує переваги локальної обробки та можливість доступу через хмару. Критичні функції виконуються локально, а аналітика, архівування чи віддалене керування — через Інтернет.

Інтеграція, безпека, захист даних:

Зі зростанням кількості пристроїв різних виробників питання інтеграції та безпеки набувають особливої ваги. Для ефективної інтеграції використовуються:

- **Гейти та шлюзи (gateway)**, які об’єднують кілька протоколів і забезпечують єдину точку входу для управління;
- **Протоколи шифрування** (TLS, SSL) для захисту даних, що передаються мережею;
- **VPN** — для безпечного віддаленого доступу до системи;
- **Багаторівнева автентифікація** — для запобігання несанкціонованому доступу;
- **Регулярне оновлення ПЗ** для закриття вразливостей та підтримки нових стандартів.

Безпека smart home включає також захист від зловмисників, запобігання атакам типу Man-in-the-Middle, безпечну передачу персональних даних та запобігання вторгненням у приватність користувачів.

Тож ринок розумного дому залишається одним із найбільш динамічних та інноваційних сегментів сучасних технологій. Щороку з’являються нові протоколи зв’язку, розширюється асортимент пристроїв, оновлюються стандарти й платформи, що разом відкривають ще більше можливостей для автоматизації, підвищення рівня безпеки, енергоефективності та комфорту мешканців.

Постійний розвиток у цій сфері стимулює виробників впроваджувати більш розумні, взаємосумісні та захищені рішення, які здатні враховувати як індивідуальні потреби користувачів, так і загальні тенденції ринку. Усе більше уваги приділяється питанням інтеграції різних пристроїв, забезпеченню захисту персональних даних, стійкості системи до кібератак і зручності користування.

1.3 Аналіз актуальних проблем

Актуальні виклики, проблеми та аналіз існуючих рішень у сфері розумного дому

Попри стрімкий розвиток технологій та зростання популярності концепції «розумного дому», впровадження подібних систем усе ще супроводжується низкою викликів, що обмежують їхнє поширення та ефективність у повсякденному житті. До ключових проблем, які сьогодні потребують уваги як з боку користувачів, так і з боку розробників, належать:

1. Проблема сумісності та фрагментації пристроїв.

Одним з найгостріших викликів є відсутність єдиного стандарту для взаємодії між пристроями різних виробників. Хоча такі ініціативи, як Matter або підтримка ONVIF для камер, намагаються створити універсальні протоколи, у реальності користувач часто стикається з ситуацією, коли новий пристрій не підтримується існуючою платформою або потребує встановлення окремого додатку. Це ускладнює централізоване керування системою, змушує користувача «жонглювати» кількома інтерфейсами, і, відповідно, знижує загальний рівень зручності та ефективності.

2. Безпека та захист персональних даних.

Інша критично важлива проблема — кібербезпека. З огляду на те, що більшість пристроїв розумного дому постійно підключені до мережі Інтернет, вони стають потенційною мішенню для зловмисників. Дослідження демонструють, що багато бюджетних smart-пристроїв мають слабке шифрування або навіть використовують за замовчуванням стандартні логіни та паролі, що значно підвищує ризик несанкціонованого доступу. Крім того, використання хмарних сервісів для зберігання даних (відеозаписів, журналів подій тощо) створює додаткові ризики витоку приватної інформації.

3. Складність налаштування та бар'єри входу.

Для технічно непідготовленого користувача налаштування системи розумного дому може виявитися надто складним. Часто виникає потреба у конфігурації мережевого обладнання, налаштуванні шлюзів, встановленні прошивок, створенні сценаріїв автоматизації тощо. У результаті навіть базові функції можуть залишитися недоступними або нерозкритими, а сам користувач — розчарованим у функціоналі.

4. Залежність від Інтернету та хмарних сервісів.

Багато комерційних систем працюють лише при наявності постійного доступу до Інтернету, що робить їх вразливими до перебоїв у мережі. У разі зникнення з'єднання, частина функцій може перестати працювати або працювати некоректно. Додатковим викликом є довгострокова надійність хмарних сервісів: у разі припинення підтримки з боку виробника або відключення серверів, пристрої можуть стати непридатними для використання.

Тепер, проналізуємо варіанти існуючих комерційних та відкритих рішень.

З метою подолання вищезазначених проблем було розроблено цілий ряд платформ для розумного дому — як комерційних, так і з відкритим кодом.

Кожне з рішень має власні переваги та недоліки, які варто враховувати при виборі архітектури системи.

1. Комерційні екосистеми

- **«Google Home» / «Nest** Google» – пропонує користувачам інтуїтивно зрозумілу систему для керування smart-пристроями через додаток Google Home. Система має гарну інтеграцію з голосовим помічником Google Assistant та підтримує велику кількість пристроїв. Проте її функціональність сильно залежить від стабільності хмарного сервісу, а користувач має обмежений контроль над внутрішньою логікою автоматизації. Крім того, розширені сценарії часто не реалізовані або потребують додаткових компонентів;

- **«Amazon Alexa»** – Подібно до Google, Amazon Alexa забезпечує керування пристроями через голосовий інтерфейс і мобільний додаток. Alexa має потужну екосистему та підтримку різних сценаріїв автоматизації (routines), проте також ґрунтується на хмарній обробці та має закритий код. Це створює складнощі для локальної автоматизації та інтеграції нестандартних рішень;

- **«Xiaomi Mi Home» / «Aqara» –** Це одна з найпоширеніших систем на ринку України завдяки відносно низькій ціні, широкому асортименту пристроїв і достатньому функціоналу. Однак Mi Home використовує закриті API, має сильну залежність від китайських серверів, а також обмежену підтримку сторонніх інтеграцій без root-доступу до хаба. У разі відсутності Інтернету більшість функцій не працюють;

- **«Apple HomeKit»** – відзначається високим рівнем безпеки, глибокою інтеграцією з пристроями Apple та підтримкою локальної автоматизації. Проте використання HomeKit можливе лише з пристроями, сертифікованими Apple, що значно обмежує вибір і збільшує вартість побудови системи.

2. Open-source платформи для розумного дому

Почнемо з «Home Assistant».

Home Assistant — одна з найпотужніших і найпопулярніших відкритих платформ для автоматизації. Вона розгортається локально на міні-ПК, сервері або навіть Raspberry Pi. Її головні переваги:

- Повна локальна робота без підключення до хмари;
- Можливість створення складних сценаріїв на основі подій, станів і умов;
- Широка сумісність: підтримка понад 2000 інтеграцій із пристроями різних виробників;
- Модульність: можна додавати кастомні компоненти, власні панелі керування, скрипти тощо.

Недоліки:

- Відносна складність налаштування для новачків — потрібне розуміння YAML, IP-мереж, MQTT;
- Висока гнучкість — водночас і плюс, і мінус: усе можна зробити вручну, але доведеться розбиратися.

Для даного проєкту ця платформа є ідеальним вибором, оскільки:

- Її легко розгорнути на наявному сервері з Linux;
- Вона підтримує інтеграцію з системами відеоспостереження;
- Можна під'єднати Zeek або аналогічні інструменти моніторингу трафіку через API/WebSocket;
- Дозволяє створювати адаптивні сценарії на основі аналізу мережевої активності.

Далі йде «OpenHAB».

OpenHAB — ще одна гнучка платформа з відкритим кодом, яка підтримує сценарії автоматизації, інтерфейси керування та інтеграцію з багатьма протоколами (Z-Wave, Zigbee, MQTT, KNX, Modbus). Основні особливості:

- Робота через Java, що забезпечує кросплатформенність;
- Широкий набір плагінів;
- Підтримка мови правил (DSL) для автоматизації.

Недоліки:

- Менш зручний інтерфейс у порівнянні з Home Assistant;
- Складніший процес налаштування автоматизацій;
- Слабша підтримка нових пристроїв.

І останні по списку: «Domoticz» / «ioBroker» / «MajorDomo».

Ці проєкти мають власні переваги:

- «Domoticz» — легкий і зручний у використанні, але з обмеженою підтримкою сучасних пристроїв.
- «ioBroker» — має найширшу інтеграцію з системами промислового рівня, але менш дружній для початківців.
- «MajorDomo» — українська/російська розробка з web-орієнтованим інтерфейсом, але слабко оновлюється.

З таким величезним набором проблем та рішень, було вирішено підійти з простої сторони та виконати усі дії нижче.

Беручи до уваги перелічені проблеми, слабкі сторони готових рішень та доступне обладнання, яке буде описано далі (зокрема — потужний сервер на базі Xeon, IP-камери, ноутбук, роутер, телефони та ТВ), доцільно реалізувати гібридну інтелектуальну систему, яка буде поєднувати переваги відкритих платформ, локального аналізу трафіку та розширеного контролю над подіями в мережі.

Проаналізувавши інформацію вище, маємо такі висновки за розділом:

У ході виконання першого розділу бакалаврської роботи було здійснено комплексний аналітичний огляд сучасного стану та перспектив розвитку інтелектуальних систем розумного дому. Проаналізовані джерела та приклади впровадження таких систем дають змогу стверджувати, що розумний дім — це не лише сукупність окремих автоматизованих рішень, а цілісна технологічна екосистема, яка здатна суттєво підвищити якість життя, забезпечити безпеку житла, раціонально використовувати ресурси та адаптуватися до поведінкових моделей мешканців.

Було встановлено, що основою функціонування подібних систем є інтеграція апаратних та програмних компонентів, об’єднаних єдиною мережею з можливістю взаємодії в режимі реального часу. Це включає в себе широке застосування протоколів зв’язку — як дротових (Ethernet), так і бездротових (Wi-Fi, Zigbee, Z-Wave, Bluetooth, Thread), а також платформних рішень, серед яких провідну роль відіграють Home Assistant, OpenHAB, Xiaomi Mi Home, Google Home, Alexa та інші.

У результаті аналізу технічних підходів було виділено дві основні архітектури — централізовану (на основі хаба) та децентралізовану (mesh-мережі з peer-to-peer комунікацією). Обидва підходи мають свої переваги: централізоване керування дає змогу швидко координувати всі пристрої через єдиний інтерфейс, у той час як децентралізована модель забезпечує більшу надійність, стійкість до збоїв та масштабованість.

Окрему увагу було приділено аналізу ключових проблем, що наразі обмежують розвиток і повсюдне впровадження smart home-систем. Передусім це:

- відсутність єдиних відкритих стандартів для взаємодії пристроїв різних виробників;
- обмежена сумісність комерційних рішень із незалежними платформами;
- залежність багатьох систем від хмарних сервісів;
- недостатній рівень захисту даних та мережевої безпеки;
- технічна складність налаштування систем для недосвідчених користувачів;
- відсутність функціональної персоналізації під специфічні сценарії побуту.

Детальний розгляд комерційних та open-source рішень дозволив виявити, що хоча більшість платних екосистем відзначаються зручністю користування та продуманим дизайном, вони, як правило, обмежені в плані конфігурації, інтеграції з «нестандартними» пристроями, а також покладаються на зовнішні сервери. Натомість платформи з відкритим кодом (зокрема Home Assistant, OpenHAB, Domoticz) дають значно більше можливостей щодо гнучкого керування, локальної обробки даних, побудови кастомних сценаріїв автоматизації, підключення додаткових модулів і забезпечення приватності користувача.

Водночас, open-source рішення потребують базових знань у галузі інформаційних технологій, роботи з мережею, скриптами та інтерфейсами, що може стати бар’єром для кінцевих користувачів.

У підсумку можна зробити висновок, що предметна область інтелектуальних систем керування будинком перебуває на стадії активного розвитку. Виявлені технічні й практичні виклики вказують на актуальність побудови гібридного рішення, що здатне працювати автономно, не залежати від зовнішніх хмар, забезпечувати високий рівень безпеки та при цьому бути адаптованим до реальних умов конкретного житлового об’єкта.

2 ПРОЕКТУВАННЯ СИСТЕМИ РОЗУМНОГО ДОМУ

2.1 Загальна архітектура системи

Основним елементом системи є високопродуктивний сервер, що виконує функцію «мозкового центру» всієї мережі. Сервер побудовано на базі процесора Intel Xeon E5 v3 з 32 ГБ оперативної пам’яті та працює під управлінням Ubuntu Server 22.04 LTS. Завдяки потужним обчислювальним ресурсам, сервер здатний у режимі реального часу обробляти великі обсяги даних, зокрема мережевий трафік, лог-файли та відеопотоки.

Всі ключові модулі системи інтегровані в єдину мережеву інфраструктуру, до якої входять:

IP-камери відеоспостереження. Чотири камери розташовано таким чином, щоб забезпечити повний охват території об’єкта. Три з них працюють у статичному режимі (моніторинг головного входу, парковки та внутрішнього двору), а одна – динамічна, здатна змінювати кут огляду залежно від умов освітлення та потреби контролю. Всі камери підтримують стандарт ONVIF, що гарантує їхню універсальну сумісність та легкість інтеграції.

Пристрої для управління та відображення інформації. У систему інтегровані смарт-телевізори, смартфони, планшети та ноутбуки. Ці пристрої дозволяють оперативно отримувати сповіщення про події, керувати сценаріями автоматизації, а також здійснювати дистанційний моніторинг і управління системою.

Мережеве обладнання. Для забезпечення надійної та швидкісної передачі даних застосовується комбінована мережа: дротове підключення за допомогою Ethernet і бездротове – через Wi-Fi. Такий підхід дозволяє оптимізувати навантаження, мінімізувати затримки та забезпечити високий рівень захищеності при обміні інформацією.

Архітектурне рішення засноване на принципі централізованого управління, коли сервер координує роботу всіх підключених пристроїв, здійснює збір і аналіз даних, а також забезпечує інтеграцію функцій відеоспостереження, моніторингу мережевого трафіку та автоматизації операцій.

Задля більшого розуміння, нижче (див. рис. 2.1) було зібрано план будинку, на якому чітко можна побачити розташування головних пристроїв в мережевій інфраструктурі, планування будинку та зони, які покриваються пристроями на кшталт маршрутизатора, камер та інших…

На рисунку 2.1 маємо такі значення:

- CAM (1-4): камери та зона їх покриття;
- Router: головний маршрутизатор мережі;
- HNAC – Home Network Analysis Computer, який аналізує трафік.

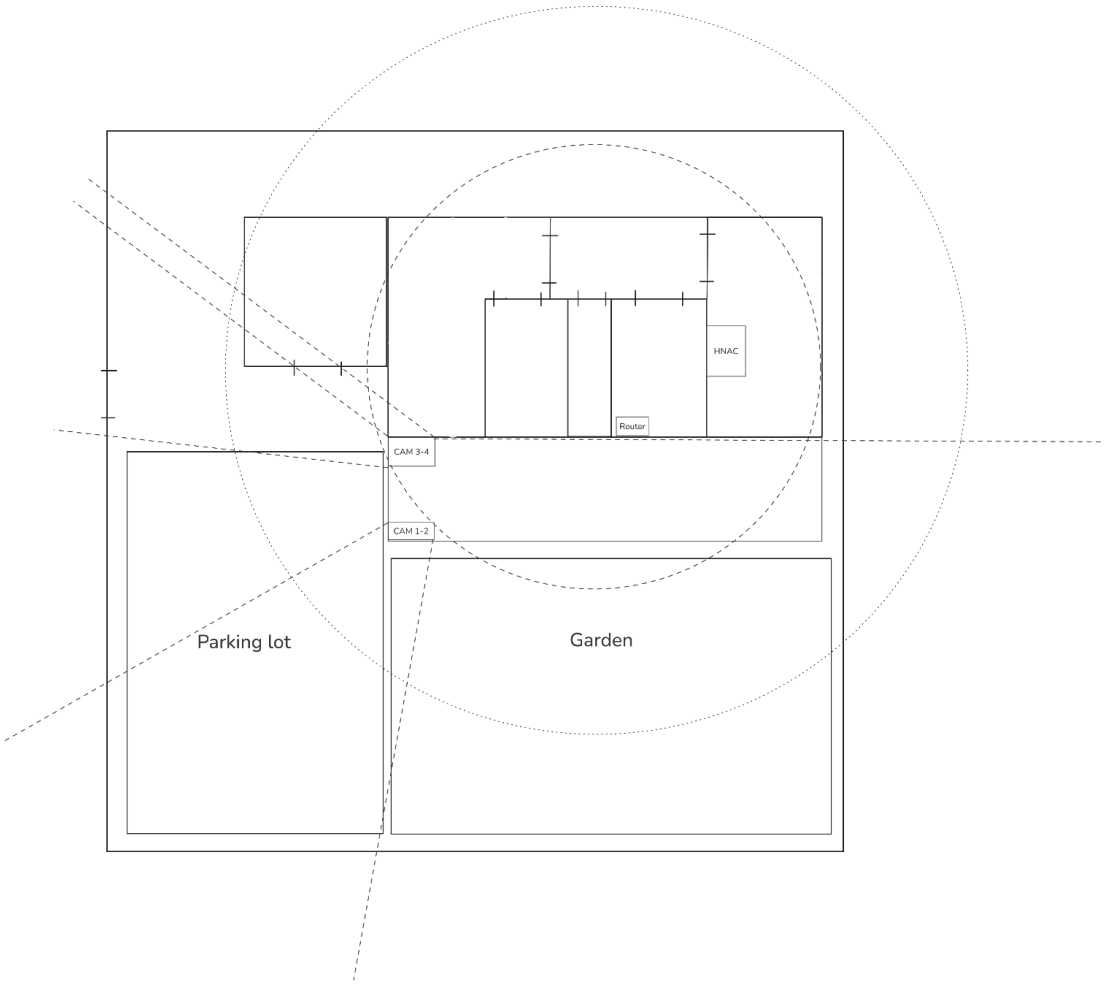

Рисунок 2.1 – План мережевої інфраструктури та будинку

Що ж стосовно апаратно-програмної інфраструктури та засобів комунікації:

Апаратна база:

Сервер, який є ядром системи, має високі технічні характеристики:

- **Процесор:** Intel Xeon E5-2670 v3, що забезпечує багатоядерну обробку завдань;
- **Оперативна пам’ять:** 32 ГБ DDR4, що гарантує швидкий обмін даними між компонентами та стабільну роботу при високому навантаженні;
- **Накопичувачі:** SSD на 240 ГБ для забезпечення високої швидкості доступу до даних у поєднанні з HDD на 500 ГБ для довгострокового зберігання лог-файлів, відеозаписів та конфігураційних файлів.

Сервер підключено до локальної мережі за допомогою провідного з’єднання Ethernet, що дозволяє забезпечити стабільну передачу даних із максимальною пропускною здатністю (до 1 Гбіт/с) і мінімізувати вплив зовнішніх електромагнітних перешкод.

Компоненти відеоспостереження та додаткові пристрої.

До складу системи входять:

IP-камери відеоспостереження.

Статичні камери: Розташовано у визначених ключових точках – головний вхід, парковка, внутрішній двір. Ці камери постійно ведуть запис відео і передають його через протокол RTSP. Дані камери можна побачити на

рисунках 2.2 та 2.3, з надписами «CAM1», «CAM2» та «CAM3».

Рисунок 2.1 – Перша та друга статичні камери

Динамічна камера: Оснащена функцією панорамування та зміни кута огляду. Завдяки власним сенсорам та алгоритмам автоматичного перемикання в нічний режим із використанням інфрачервоного підсвічування, ця камера демонструє високу ефективність у змінних умовах освітлення, і побачити яку можна на рисунку 2.2, зліва.

Рисунок 2.2 – Статична та динамічна камери

Інтегровані пристрої управління. Смарт-телевізори, смартфони, планшети та ноутбуки використовуються для відображення сповіщень, дистанційного керування системою та оперативного моніторингу подій. Ця взаємодія забезпечує простий доступ до всіх функцій розумного дому і дозволяє користувачу взаємодіяти з системою у реальному часі.

Додаткові датчики та виконавчі пристрої. Для підвищення безпеки та автономності системи інтегровано:

Програмне забезпечення та засоби передачі даних.

Для поставленої задачі самий раціональний вибір був Suricata як основний засіб аналізу мережевого трафіку. Обумовлено це її високою продуктивністю, широкими можливостями конфігурації та адаптивністю до сучасних загроз. У порівнянні з аналогічними IDS/IPS-рішеннями, Suricata пропонує багатопотокову обробку даних, що дозволяє ефективно розподіляти навантаження між ядрами процесора. Враховуючи, що центральний сервер системи оснащений продуктивним Xeon з великою кількістю потоків, використання Suricata дозволяє максимально повноцінно використати апаратні ресурси для аналізу великого обсягу трафіку без затримок.

Додатковим фактором є її гнучкість у налаштуванні правил фільтрації. Suricata підтримує формат сигнатур Snort та має можливість імпортувати великі відкриті бази даних загроз, зокрема Emerging Threats. Це дозволяє виявляти не лише стандартні атаки (сканування портів, DoS-атаки, аномалії DNS-запитів), але й специфічні загрози, які можуть бути спрямовані саме на IoT-пристрої або внутрішню мережу розумного дому.

Важливою перевагою Suricata є її розширена система логування. Вона підтримує запис подій у форматах fast.log та eve.json, що забезпечує можливість їх подальшого аналізу через аналітичні платформи типу Kibana, Grafana або SIEM-системи. Це особливо важливо для побудови гнучкої системи моніторингу, яка не просто фіксує загрози, але й дозволяє візуалізувати тенденції, виявляти поведінкові аномалії та передбачати потенційні загрози.

Не менш вагомим є факт, що Suricata є рішенням із відкритим кодом, яке має активну спільноту розробників. Це гарантує регулярне оновлення правил безпеки, підтримку сучасних архітектур та своєчасну адаптацію до нових викликів у сфері кіберзахисту. Для системи розумного дому критично важливо мати інструмент, який залишається актуальним, здатним швидко реагувати на зміну сценаріїв атак та зберігати свою ефективність у довгостроковій перспективі.

Саме ці причини визначили вибір Suricata як базового рішення для аналізу трафіку і побудови системи реагування на загрози в інтелектуальній інфраструктурі розумного дому. Це поєднання продуктивності, широких можливостей конфігурації, аналітичного потенціалу та гнучкості масштабування, яке забезпечує стабільну та безпечну роботу всієї системи.

Suricata також має важливу особливість – можливість роботи не лише в режимі аналізу трафіку, а й у режимі попередження загроз, що дозволяє реалізувати систему активного захисту. Це означає, що при виявленні аномалій система може не просто зафіксувати інцидент, а й миттєво реагувати, блокуючи небажаний трафік або ізолюючи підозрілі пристрої. Такий підхід значно підвищує рівень безпеки розумного дому, мінімізуючи ризики компрометації внутрішньої мережі.

2.3 Розробка логіки сценаріїв реагування

Сучасні системи розумного дому повинні не лише збирати інформацію, але й оперативно реагувати на всі потенційні загрози та нештатні ситуації. Основним завданням розробки логіки реагування є створення багаторівневої системи, що здатна аналізувати мережевий трафік, порівнювати його з попередньо заданими правилами та без зволікань ініціювати відповідні заходи для мінімізації ризиків. Саме це спрямування дозволяє досягнути високої ефективності виявлення аномалій та захисту як внутрішнього мережевого простору, так і підключених IoT-пристроїв.

Аналіз та класифікація подій.

На центральному сервері, обладнаному платформою Suricata, відбувається постійний моніторинг трафіку. Система аналізує всі пакети, що проходять через мережу, і використовує велику базу правил, зокрема ті, що отримані з відкритих репозиторіїв (наприклад, Emerging Threats). В процесі аналізу визначаються такі категорії подій:

Порт-сканування. Якщо система виявляє серію запитів до великої кількості портів із одного джерела, це автоматично класифікується як ймовірна спроба порт-сканування.

Аномальні DNS-запити. Раптовий сплеск DNS-відповідей або звернень до невідомих доменів може свідчити про спробу компрометації або використання ботнетів.

Незвичайна поведінка протоколів (TCP, ICMP). Значне відхилення в кількості SYN або ICMP пакетів може бути ознакою DoS-атаки або інших типів зловмисного трафіку.

Побудова сценаріїв реагування.

Для кожного типу виявленої аномалії розроблено набір сценаріїв реагування, який включає як автоматизовані, так і ручні дії оператора. Сучасна система розумного дому повинна працювати за принципом «реагуй негайно або логуй надалі», що дозволяє мінімізувати будь-які затримки при реагуванні.

Сценарій реагування на порт-сканування:

Автоматичне логування: Під час виявлення підозрілих запитів система негайно записує детальну інформацію: IP-адресу джерела, часову мітку, кількість та тип запитів.

Блокування трафіку: За потреби система може автоматично внести IP-адресу у чорний список за допомогою налаштованих правил фаєрволу.

Сценарій реагування на аномальні DNS-запити:

Фіксація всіх DNS-запитів та відповідей із зазначенням доменних імен.

Аналіз шаблонів: На основі зібраних даних система ідентифікує повторювані сплески або незвичні шаблони, що характеризують підозрілу активність.

Ізоляція пристрою: У випадку, якщо виявлено пристрій з аномальними запитами, система може ініціювати тимчасове ізолювання даного вузла із загальної мережі.

Сценарій реагування на DoS-атаки та аномалії мережевого трафіку:

Моніторинг трафіку: Постійний аналіз кількості ICMP або SYN пакетів дозволяє виявляти раптове зростання навантаження, яке може бути ознакою DoS-атаки чи інших аномалій. Завдяки безперервному спостереженню за нормальними показниками мережевого руху, система може оперативно визначати відхилення від стандартних параметрів.

Регулювання пропускної здатності: Автоматичне коригування параметрів мережі для певних IP-адрес або груп вузлів, що виявилися під загрозою, може зменшити вплив атаки. Це дозволяє розподілити мережеве навантаження більш рівномірно та запобігти блокуванню критично важливих сервісів, забезпечуючи при цьому збереження доступності внутрішніх ресурсів.

Аварійне сповіщення: Інтегроване сповіщення надсилається оператору, що дає можливість оперативно вжити заходів із залученням додаткових кібербезпекових модулів. Система може сповіщати як за допомогою push-повідомлень, так і через спеціально налаштований Telegram-бот, що забезпечує швидкий обмін інформацією про поточний стан мережі.

Інтеграція та автоматизація процесів реагування: Розроблена логіка сценаріїв реагування не обмежується лише фіксацією та сповіщенням. Важливим є інтегрування системи з іншими високотехнологічними компонентами інфраструктури розумного дому, що забезпечує комплексний підхід до моніторингу та запобігання загрозам.

Інтеграція з системою автоматизації Home Assistant: При виявленні загроз автоматично можуть активуватися сценарії, що змінюють режим роботи будинку. Наприклад, під час виявлення підозрілої активності система відеоспостереження може автоматично увімкнути зовнішнє освітлення, активувати сигналізацію або навіть заблокувати доступ до певних сегментів мережі, забезпечуючи оперативну реакцію без участі оператора.

Аналітика та історична обробка даних: Всі події зберігаються у вигляді структурованих логів (у форматі JSON або YAML), що дозволяє їх подальший аналіз за допомогою систем візуалізації даних. Це створює можливість побудови дашбордів, які відображають динаміку загроз, часові інтервали нападів та статистичні показники, що допомагає у прогнозуванні потенційних атак та удосконаленні правил реагування.

Додатково, особлива увага приділяється постійному тестуванню та адаптації сценаріїв реагування. На основі зібраних лог-файлів та аналізу статистичних даних адміністраторам регулярно проводиться переоцінка правил фільтрації. Це дозволяє оперативно коригувати параметри системи відповідно до змін у поведінці мережевого трафіку, що в свою чергу підвищує загальну ефективність захисту.

Ще одним важливим аспектом є інтеграція всієї системи в єдину екосистему розумного дому, де всі компоненти взаємодіють для забезпечення максимального захисту. Це дозволяє створити умовний «цинк захисту», в якому кожна зафіксована аномалія розглядається в контексті загальної карти безпеки системи.

2.4 Розробка логіки системи, сценарії, потоки та інше

Розробка логіки системи, її сценаріїв та управліньских потоків є центральним етапом створення інтегрованої інфраструктури розумного дому. Основна мета цього підходу полягає у забезпеченні безперебійного збору, аналізу та обробки даних, що надходять із різних джерел – датчиків, IP – камер, серверних модулів та інших IoT-пристроїв. Кожен компонент системи працює у взаємодії з іншими, що дозволяє як оперативно реагувати на надзвичайні події, так і вести постійний моніторинг стану мережевого середовища.

Основою побудови логіки є модульний підхід, за яким кожен функціональний блок має чітко визначені входи та виходи даних. Наприклад, інформаційні потоки від датчиків руху, температури чи вологості надходять до централізованого процесора, де вони нормалізуються та аналізуються. Потім, ці дані агрегруються в структурованих логах (у форматі JSON або YAML) і передаються до аналітичних блоків. Це дозволяє не лише виявляти порушення у роботі системи, але й створювати історичні звіти, що в майбутньому служитимуть основою для оптимізації та самоаналізу модулів.

Окремо, варто відзначити, що логіка системи включає як компоненти фіксації подій, так і розгалужені сценарії реагування. Наприклад, при виявленні підозрілої активності з IP – камери, система генерує подію й автоматично передає інформацію до центрального блоку управління. За допомогою інтеграції з платформою Home Assistant запускаються відповідні сценарії – це може бути активація зовнішнього освітлення, увімкнення сигналізації або блокування доступу до певних мережевих сегментів. Такий підхід забезпечує не тільки швидке реагування, але й адаптивність до змін у зовнішньому середовищі.

Для обробки вхідних даних використовуються алгоритми, що аналізують як потоки в режимі реального часу, так і збережені історичні логи. За допомогою сучасних IDS/IPS-рішень, логічна структура системи дозволяє порівнювати отриману інформацію з заздалегідь визначеними шаблонами аномалій. Часто алгоритми обчислюють показники, такі як частота певних подій, кількість помилок передачі або незвичайні патерни, що спричиняють відхилення від нормальної роботи системи. Таким чином, кожна подія ретельно класифікується, що дозволяє забезпечити високу точність і оперативність реагування.

Таким чином, розробка логіки системи, сценаріїв реагування та управлінських потоків є комплексним процесом, який забезпечує ефективну взаємодію всіх компонентів розумного дому. Цей підхід гарантує оперативний аналіз і обробку даних, швидке виявлення потенційних загроз і своєчасну адаптацію функціональності системи до змін у середовищі. Використання діаграм, схем та фотоматеріалів є важливим інструментом для ілюстрації процесів, що ще більше підвищує зрозумілість і наочність кожної складової цієї моделі.

3 РЕАЛІЗАЦІЯ ОСНОВНИХ КОМПОНЕНТІВ СИСТЕМИ

3.1 Реалізація моніторингу мережевого трафіку

У сучасних умовах розвитку цифрових технологій та Інтернету речей (IoT) безпека локальної мережі та ефективний моніторинг її трафіку набувають надзвичайного значення. Для систем розумного дому, де безліч пристроїв взаємодіють між собою, навіть незначне відхилення від норми може бути сигналом про потенційну атаку чи порушення безпеки. Реалізація моніторингу мережевого трафіку є комплексним процесом, який передбачає збори даних із численних джерел, їх попередню обробку, класифікацію та адаптивне реагування. У цьому підрозділі докладно розглядаються технічні рішення, алгоритмічні підходи та практичні аспекти впровадження системи, побудованої на базі високопродуктивного серверного обладнання та спеціалізованого програмного забезпечення, зокрема Suricata.

Розумний дім – це не просто набір IoT-пристроїв, а інтегрована система з багаторівневим захистом, де кожен компонент відіграє свою роль у забезпеченні цілісності мережевого простору. Центральним елементом є сервер із високими обчислювальними потужностями, обладнаний сучасним процесором Intel Xeon з багатьма ядрами. Завдяки великій оперативній пам’яті та швидким зберігачам даних (комбінація SSD і HDD), система здатна в режимі реального часу обробляти величезні обсяги мережевого трафіку.

Для моніторингу та аналізу даних використовується система Suricata – потужне IDS/IPS-рішення, яке працює в багатопоточному режимі. Suricata здійснює аналіз кожного пакету, що проходить через мережу, порівнюючи його з великою базою відомих шаблонів та правил. Це дозволяє як фіксувати стандартні загрози (наприклад, порт-сканування, DoS-атаки), так і виявляти аномалії у мережевому дії, що не входять до базових сценаріїв.

Однією з ключових переваг використання Suricata є її здатність записувати події у різних форматах (наприклад, JSON або YAML). Це дозволяє легко інтегрувати дані з системами візуалізації, такими як Grafana чи Kibana, щоб оперативно аналізувати інформацію через зручні дашборди. Важливість такої інтеграції полягає в можливості швидко визначити моменти збільшення навантаження, географічний розподіл атакуючих IP-адрес, часові інтервали нападів та інші критичні показники, що є надзвичайно цінними під час прийняття рішень щодо захисту мережі.

У процесі роботи системи основна увага приділяється аналізу мережевого трафіку за допомогою алгоритмів, які виконують кілька етапів обробки даних:

Збір даних та первинна обробка. Всі мережеві потоки, що надходять із IP-камер, датчиків та інших IoT-пристроїв, збираються через центральний комутатор або маршрутизатор і надходять до серверного модуля. На цьому етапі інформація може бути попередньо агрегована для зниження обсягу даних, що надходять у систему аналізу. При цьому використовуються стандартні мережеві протоколи (TCP/IP, Ethernet, Wi-Fi, RTSP, ONVIF), що гарантують сумісність і високий рівень надійності з'єднання.

Детальний аналіз із застосуванням правил. Suricata порівнює кожен пакет з базою відомих загроз і аномалій. При цьому відбувається класифікація даних за категоріями: порт-сканування, аномальні DNS-запити, нестандартні патерни інтернет-трафіку (включаючи незвичну кількість SYN, ICMP пакетів тощо). Кожне відхилення від норми фіксується із зазначенням повної інформації: IP-адреса, порт, часовий штамп, тип аномалії.

Побудова логів та збереження даних. Зібрані дані зберігаються у вигляді структурованих логів, що дозволяє проводити як оперативний, так і історичний аналіз. Така база даних є основою для подальшої аналітики, а також для розробки методів машинного навчання, які можуть передбачати нові загрози на основі історичних трендів.

Візуалізація та аналітика. За допомогою інтегрованих систем візуалізації даних, таких як Grafana чи Kibana, оператор може отримати повноцінне уявлення про поточний стан мережевого середовища. Дашборди дозволяють відслідковувати не тільки поточні показники, але й аналізувати тенденції за допомогою графіків, діаграм та таблиць. Наприклад, зміни у кількості мережевих запитів можуть бути представлені у вигляді часових рядів, що демонструють зростання кількості аномалій у визначені періоди.

Реалізація системи реагування та інтеграція з платформами автоматизації

Система розумного дому, окрім пасивного моніторингу, повинна мати здатність оперативно реагувати на виявлені загрози. Саме тому окрім алгоритмів обробки мережевого трафіку, значна увага приділяється створенню потужних сценаріїв реагування, що інтегровані з іншими компонентами інфраструктури.

Автоматизоване реагування за допомогою інтегрованого повідомлення. При виявленні підозрілої активності система негайно генерує сповіщення, що надсилаються через різноманітні канали – push-повідомлення, email, або спеціально налаштовані Telegram-боти. Ці повідомлення містять детальну інформацію про інцидент, що дозволяє оператору миттєво прийняти рішення щодо подальших дій.

Сценарії автоматичного контролю. Інтеграція з платформою Home Assistant дозволяє запускати складні автоматизовані сценарії, коли виявлено загрозу. Наприклад, при реєстрації незвичного потоку відео або підвищеній активності мережевого трафіку, система може автоматично активувати зовнішнє освітлення, сигналізацію або зупинити роботу певних вузлів мережі. Ці сценарії не лише зменшують час реакції, але й допомагають запобігти подальшому розповсюдженню загрози.

Динамічне регулювання параметрів мережі. Система може автоматично коригувати пропускну здатність для виявлених під загрозою пристроїв. Наприклад, у разі атаки типу DoS (Denial of Service) система застосовує алгоритми балансування навантаження, що дозволяють зменшити вплив атаки через розподілення трафіку між декількома каналами. Таке регулювання забезпечує збереження загального рівня безпеки та доступності сервісів незалежно від зовнішнього навантаження.

Історична обробка даних та прогноз загроз. Зберігання логів у структурованих форматах відкриває можливості для подальшої аналітики з використанням методів машинного навчання. Аналізуючи історичні дані, система може виявити закономірності, які вказують на потенційні майбутні загрози, і адаптувати критерії реагування. На практиці це дозволяє створити адаптивну систему, яка з часом стає більш ефективною у виявленні та запобіганні рідкісним атакам.

Масштабованість та модульність системи.

Еволюція системи розумного дому неминуче передбачає її масштабування та інтеграцію з додатковими IoT-пристроями. Основною перевагою розробленої архітектури є її модульність, що дозволяє додавати нові підсистеми без кардинальної перебудови базової інфраструктури.

Підключення нових пристроїв: Завдяки використанню стандартних протоколів зв’язку (TCP/IP, Ethernet, Wi-Fi, ONVIF, RTSP) система легко інтегрує додаткові камери, датчики руху, температури, вологості та інші пристрої. Розширення функціоналу не потребує додаткової складної налаштування, оскільки всі пристрої працюють у єдиній мережевій екосистемі.

Універсальність розгортання: Завдяки тому, що базова архітектура передбачає використання відкритих API і стандартних протоколів, існує можливість створення універсальних образів системи – наприклад, у вигляді Docker-контейнерів або ISO-образів. Це значно спрощує процес розгортання системи як у приватних будинках, так і в комерційних об'єктах, забезпечуючи швидкий старт та мінімальні витрати часу на налаштування нових об’єктів.

Інтеграція з SIEM-системами: Для подальшої автоматизації аналізу та централізованого моніторингу безпеки планується інтегрування з SIEM-платформами, що дозволить збирати і аналізувати дані з численних будинків або підприємств. Такий підхід дозволить не тільки виявляти регіональні загрози, а й адаптувати політики безпеки для всієї мережі об'єктів, оптимізуючи заходи захисту.

Практичні аспекти впровадження та управління.

На практиці реалізація системи моніторингу мережевого трафіку здійснюється у декілька етапів. Спершу проводиться проведення аудиту існуючої інфраструктури, включаючи оцінку пропускної здатності мережі, поточних сценаріїв взаємодії пристроїв та рівня безпеки. На основі цього розробляються індивідуальні налаштування для кожного компоненту.

Після первинної інтеграції проводиться тестування системи на різних сценаріях: від моделювання типових атак до симуляції раптових зростань навантаження. Ці тестові сесії дозволяють налаштувати пороги сповіщення, оптимізувати алгоритми обробки даних і впевнитися у правильності роботи всіх модулів. Результати тестування документуються у вигляді детальних звітів, що містять таблиці, графіки та діаграми. Завдяки цьому адміністратори отримують можливість оперативно коригувати налаштування та впроваджувати рекомендації з покращення продуктивності.

Окрім цього, впровадження системи супроводжується регулярним навчанням операторів та оновленням баз даних загроз. Це дозволяє підтримувати актуальність програмного забезпечення та забезпечує безперебійний захист мережевого середовища за умов постійно зростаючих вимог до кібербезпеки.

Застосування багаторівневого моніторингу мережевого трафіку, розгорнута обробка лог-файлів із використанням Suricata, а також інтеграція з сучасними аналітичними та автоматизаційними платформами створюють надійну основу для забезпечення безпеки розумного дому. Система здатна не лише оперативно реагувати на загрози, але й адаптуватися до змін у мережевому середовищі за рахунок автоматичного аналізу і масштабування. Такий комплексний підхід дозволяє знизити ризики несанкціонованого доступу, зберегти цілісність інформації та забезпечити постійну готовність до протидії новим кіберзагрозам.

З огляду на описані технології та практичні кейси впровадження, система спрямована на досягнення високої продуктивності, гнучкості та масштабованості. Реалізація даної логіки забезпечує як оперативний контроль над поточним станом мережевого трафіку, так і довгострокову аналітику, що дозволяє удосконалювати правила реагування та впроваджувати інноваційні технології з метою передбачення майбутніх загроз.

Таким чином, реалізація моніторингу мережевого трафіку та виявлення підозрілих активностей виступає як фундаментальна складова системи розумного дому. Об’єднання потужних апаратних рішень, спеціалізованого програмного забезпечення та сучасних аналітичних методів забезпечує не лише безперервний збір та детальний аналіз даних, а й дозволяє оперативно реагувати на потенційні загрози за допомогою інтегрованих автоматизованих сценаріїв.

У свою чергу, масштабованість системи гарантує її адаптацію до зростаючих потреб і умов, що робить її життєздатним та перспективним рішенням для широкого спектру застосувань у сфері безпеки розумного дому. Крім цього, завдяки можливості інтегрувати додаткові датчики та IoT-пристрої, система може розширювати свої функціональні можливості відповідно до специфіки об’єкта й змін у цифровому середовищі. Регулярне оновлення програмного забезпечення та адаптація аналітичних алгоритмів забезпечують високий рівень захисту навіть у разі виникнення нових типів загроз, що робить рішення ще більш надійним та ефективним.

3.2 Опис налаштування інтеграції відеонагляду

У проєкті реалізовано використання чотирьох камер відеоспостереження, що є одним із ключових компонентів системи, спрямованих на забезпечення безпеки об’єкта. Три з камер є статичними, тобто вони встановлені на фіксованих точках і не мають функції зміни кута огляду, що дозволяє чітко контролювати основні входи, коридори чи інші критично важливі зони. Одна ж камера є динамічною – вона має можливість панорамування та нахилу, що дозволяє коригувати її поле огляду у відповідності до поточних умов і забезпечує гнучкість при реагуванні на непередбачені ситуації.

Усі камери підключено до мережі за допомогою Wi-Fi, що робить їх розташування більш гнучким, оскільки немає необхідності прокладати кабелі до кожного об’єкта. При цьому кожна камера орієнтована на конкретну зону спостереження – це дозволяє оптимально розподілити зону контролю та забезпечити максимальну покритість території. Система підтримує інтеграцію із серверним обладнанням, завдяки чому дані, що надходять від камер, миттєво обробляються центральною системою моніторингу.

Щодо налаштування камер, то три із чотирьох пристроїв налаштовуються безпосередньо через комп’ютер, до якого вони підключені. Для цього використовується спеціальне програмне забезпечення, яке надає можливість регулювати основні параметри роботи: чіткість зображення, роздільну здатність, частоту кадрів, а також встановлювати режими роботи для денного й нічного спостереження. Завдяки такому підходу адміністратор системи має можливість детально налаштувати кожну камеру відповідно до специфіки використовуваної зони – наприклад, для камери, що фіксує головний вхід, можна задати високий рівень роздільної здатності й оптимальні параметры освітлення.

Відмінністю четвертої, динамічної камери, є спосіб її налаштування, який здійснюється через веб-інтерфейс. За допомогою введення локального IP-адресу в браузер користувач отримує доступ до системи налаштувань цієї камери. Такий підхід дозволяє оперативно вносити зміни – корегувати налаштування панорамування, регулювати кут огляду, а також оновлювати програмне забезпечення прямо з веб-інтерфейсу. Гнучкість даного методу забезпечує зручність управління камерами з різних пристроїв, що є важливим фактором у випадку, коли потрібна оперативна реакція на зміну умов спостереження.

Інтеграція всіх чотирьох камер у єдину мережеву систему дозволяє автоматизувати процес збору та передачі відеоданих до центрального серверу. Це забезпечує можливість об'єднання потоків з усіх камер у єдину систему аналізу, що не лише спрощує моніторинг, але й дає змогу реалізувати складні сценарії реагування, наприклад, автоматичне переключення між режимами роботи камер у випадку виявлення підозрілої активності. Подібна інтеграція також дозволяє проводити глибокий аналіз історії спостережень, що є основою для оптимізації параметрів роботи кожного пристрою окремо.

Завдяки використанню бездротової технології Wi-Fi, система набуває додаткової гнучкості – камери можна розташовувати у важкодоступних місцях або там, де прокладання мережевого кабелю є неможливим чи надто витратним. Це дозволяє створити більш адаптивну систему, що охоплює усі критично важливі зони об’єкта, зменшуючи сліпі точки та підвищуючи загальний рівень безпеки. Спеціальні алгоритми програмного забезпечення допомагають оптимізувати передачу даних, забезпечуючи стабільність сигналу навіть в умовах високого навантаження на мережу.

Отже, докладна настройка камер, як через комп’ютер, так і через веб-інтерфейс локального IP, є невід’ємною частиною функціональної складової системи розумного дому. Така гнучка схема налаштування дозволяє максимально ефективно використовувати кожну камеру, забезпечуючи стабільний моніторинг, оперативну реакцію на потенційні загрози та формуючи базу для подальшої інтеграції з іншими компонентами системи.

У системі розумного дому, де всі пристрої, зокрема відеокамери, підключені до мережі через Wi-Fi, забезпечення захисту каналів зв’язку та виявлення спроб несанкціонованого доступу має першорядне значення. Suricata, як потужний IDS/IPS, виступає ключовим елементом даної системи безпеки, адже вона здійснює постійний моніторинг мережевого трафіку, аналізуючи кожен пакет даних, що проходить через мережу. Завдяки своїм можливостям у багатопотоковій обробці даних, Suricata здатна оперативно виявляти навіть найдрібніші аномалії у потоках, що надходять від камер, в тому числі й спроби зламати протоколи зв’язку, використовувані для передачі відео.

Особливо критичною є безпека динамічної камери, яка налаштовується через веб-інтерфейс за локальним IP. Вона, як і статичні пристрої, є потенційним об’єктом атак, оскільки підключення через Wi-Fi створює додаткові вектори для зловмисних дій. Suricata відстежує будь-які незвичні запити, спрямовані до веб-інтерфейсу цієї камери, аналізує спроби несанкціонованого доступу або маніпуляцій із параметрами налаштування, що дозволяє вчасно сигналізувати про потенційні загрози та активувати заходи протидії.

Окрім виявлення атак на рівні веб-інтерфейсів, Suricata ефективно контролює мережевий трафік, пов’язаний з протоколами RTSP і ONVIF, які використовуються для передачі відео. Вона здатна розпізнавати підозрілі зміни у форматі потоків, нетипову кількість запитів або аномальні сплески трафіку, що можуть свідчити про спроби DoS-атак або зловмисну маніпуляцію даними камери. Таким чином, Suricata допомагає гарантувати, що лише легітимний трафік надходить до серверів системи, а всі потенційні загрози миттєво блокуються або передаються оператору для подальшого аналізу.

Інтеграція Suricata в систему розумного дому забезпечує не лише виявлення та попередження атак, а й ведення детального логування мережевих подій. Зібрані дані допомагають адміністраторам аналізувати історію діяльності мережі, виявляти закономірності та розробляти стратегії запобігання новим загрозам.

3.3 Реалізація управління пристроями в мережі

Сервера основного управління розумним домом працює під управлінням Ubuntu Server, що дозволяє використовувати потужні засоби командного рядка для адміністрування мережевого середовища. Центральним завданням цього сервера є забезпечення централізованого контролю над IoT-пристроями, а також можливість оперативного реагування на зміну стану мережі за допомогою стандартних і спеціалізованих інструментів.

Налаштування серверу і віддаленого доступу

Після встановлення Ubuntu Server 22.04 LTS першочергово проводиться оновлення системи:

bash

```
sudo apt update && sudo apt upgrade -y
```

Для віддаленого адміністрування встановлюється та налаштовується SSH-сервіс. Щоб перевірити статус сервісу, виконайте:

bash

```
sudo systemctl status ssh
```

Якщо SSH не встановлено, його можна встановити командою:

bash

```
sudo apt install openssh-server
```

З метою підвищення безпеки стандартний порт SSH замінюється на нестандартний. Для цього відкрийте файл конфігурації:

bash

```
sudo nano /etc/ssh/sshd_config
```

Знайдіть рядок, що містить `Port 22` і змініть його, наприклад, на:

```
Port 2222
```

Після збереження файлу перезапустіть SSH-сервіс:

bash

```
sudo systemctl restart ssh
```

Налаштування мережевого захисту за допомогою UFW

Для обмеження доступу до серверу та контролю мережевих з'єднань використовується UFW (Uncomplicated Firewall). Якщо UFW ще не встановлено, зробіть це командою:

bash

```
sudo apt install ufw
```

Після встановлення увімкніть UFW:

bash

```
sudo ufw enable
```

Додайте правило для дозволу трафіку на новий порт SSH:

bash

```
sudo ufw allow 2222/tcp
```

За потребою, можна відкрити додаткові порти для інших сервісів (наприклад, HTTP та HTTPS):

bash

```
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
```

Перевірте статус UFW, щоб впевнитися, що всі правила застосовано:

bash

```
sudo ufw status verbose
```

Управління мережевим трафіком за допомогою iptables

Для більш точного налаштування доступу до мережі та управління пристроями використовується iptables. За допомогою цього інструменту можна створювати правила для блокування або обмеження з'єднань з конкретними IP-адресами. Наприклад, щоб заблокувати доступ для пристрою з IP-адресою 192.168.0.100, виконайте:

bash

```
sudo iptables -A INPUT -s 192.168.0.100 -j DROP
```

Щоб змінені правила зберігалися після перезавантаження, встановіть пакет iptables-persistent:

bash

```
sudo apt install iptables-persistent
```

Централізоване управління пристроями та автоматизація

За допомогою створення скриптів та API-інтерфейсів адміністратор може віддалено керувати підключенням, відключенням або обмеженням доступу пристроїв у мережі. Наприклад, для автоматизації процесу блокування підозрілих IP-адрес можна написати невеликий Bash-скрипт:

bash

```
#!/bin/bash
# Скрипт для блокування IP-адреси

if [ -z "$1" ]; then
  echo "Будь ласка, вкажіть IP-адресу для блокування."
  exit 1
fi

sudo iptables -A INPUT -s $1 -j DROP
echo "IP-адреса $1 заблокована."
```

Збережіть цей скрипт, наприклад, як `block_ip.sh`, і зробіть його виконуваним:

bash

```
chmod +x block_ip.sh
```

Таким чином, ви зможете, викликаючи цей скрипт із зазначенням IP-адреси, швидко реагувати на виявлену підозрілість.

Керування підключенням пристроїв через DHCP і VLAN

Щоб централізовано управляти пристроями, які підключаються до мережі, можна налаштувати DHCP-сервер для присвоєння постійних IP-адрес зарезервованим пристроям. Файл конфігурації DHCP-сервера (наприклад, `/etc/dhcp/dhcpd.conf`) дозволяє визначити статичні адреси для важливих компонентів системи. За допомогою VLAN можна розділити мережу на окремі сегменти для підвищення безпеки та оптимізації трафіку.

Наприклад, для створення окремої VLAN-групи для камер і іншої для IoT-пристроїв можна використовувати конфігурацію в Netplan:

yaml

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp3s0:
      dhcp4: no
  vlans:
    vlan10:
      id: 10
      link: enp3s0
      addresses: [192.168.10.2/24]
```

Такий підхід дозволяє ізолювати відеокамери від інших пристроїв, знижуючи ризик компрометації всієї мережевої інфраструктури.

Автоматизація управління через веб-інтерфейс

Для зручності адміністрування можна розгорнути веб-додаток, написаний на базі фреймворків, таких як Django або Flask, що працюватиме як API для керування пристроями. За допомогою цього додатку адміністратор може отримувати інформацію про поточний стан мережі, управляти підключеними пристроями, примінювати налаштування UFW чи iptables, а також створювати завдання для автоматичного реагування у разі виявлення загроз.

Приклад API-виклику для керування пристроями на Python може виглядати наступним чином:

python

```
import subprocess

def block_ip(ip_address):
    command = f'sudo iptables -A INPUT -s {ip_address} -j DROP'
    subprocess.run(command, shell=True, check=True)
    return f"IP {ip_address} заблоковано."

# Виклик функції
print(block_ip("192.168.0.100"))
```

Запровадження такого API дозволяє створити централізовану систему управління, яка в режимі реального часу контролюватиме стан пристроїв у мережі та забезпечуватиме їх захист.

Висновки:

Таким чином, реалізація управління пристроями в мережі на базі Ubuntu Server включає комплексне налаштування серверного обладнання, забезпечення безпечного віддаленого доступу через SSH, налаштування мережевого брандмауера UFW, точне керування трафіком за допомогою iptables та автоматизацію процесів управління.

3.3 Реалізація взаємодії користувача із системою

Основною метою взаємодії користувача із системою є забезпечення зрозумілого, інтуїтивного та гнучкого механізму управління всіма компонентами розумного дому. Система побудована таким чином, що будь-який адміністратор або кінцевий користувач може оперативно отримувати доступ до центрального серверу, аналізувати поточний стан мережі, переглядати історію подій і здійснювати необхідні налаштування через зручний інтерфейс.

Для цього розроблено багаторівневу архітектуру взаємодії, що включає як веб-додатки, так і мобільні та настільні клієнти. Веб-інтерфейс, розгорнутий на основі сучасних фреймворків, дозволяє у режимі реального часу відображати статистичні дані, графіки із змінами мережевого трафіку, а також детальні звіти про всі події, зафіксовані системою. Адміністратор може через цей інтерфейс переглядати логи, аналізувати ситуації за допомогою візуальних дашбордів, а також використовувати інтерактивні елементи управління для виконання дій, таких як блокування пристроїв або зміна параметрів автоматизованої відповіді.

За допомогою спеціально розробленого API, яке працює на сервері з Ubuntu, користувач отримує можливість віддаленого керування мережевими пристроями через прості HTTP-запити. Наприклад, за допомогою наступної команди можна отримати поточний стан системи:

bash

```
curl -X GET http://<IP_СЕРВЕРА>:<PORT>/api/status
```

Це дозволяє не лише швидко отримувати інформацію, але і інтегрувати систему з іншими порталами або мобільними додатками. Серед функцій, реалізованих через API, є можливість відправлення команд для зміни налаштувань пристроїв, перевірка стану безпеки, а також ініціація скриптів, що блокують підозрілі з’єднання за допомогою iptables.

Користувач також може використовувати командний рядок безпосередньо для перегляду логів на сервері. Наприклад, перегляд останніх рядків системних логів здійснюється командою:

bash

```
tail -f /var/log/syslog
```

Аналогічно, для отримання інформації про мережевий стан застосовуються команди на зразок:

bash

```
ifconfig
netstat -tulnp
```

Ці команди допомагають адміністратору у режимі реального часу контролювати активність мережі, виявляти проблемні IP-адреси та аналізувати з’єднання, що є важливим етапом у процесі керування системою.

Особливу увагу приділено інтуїтивній організації користувацького інтерфейсу, завдяки якому навіть людина з базовими навичками може швидко орієнтуватися у функціях системи. Веб-додаток містить логічно структуровані розділи, у яких відображаються основні показники системи, такі як активність

пристроїв, історія подій, рівень навантаження на мережу, а також сповіщення про критичні зміни. Ці дані наочно демонструються у вигляді графіків, діаграм та таблиць, що дозволяє швидко приймати рішення.

Важливо також, що система передбачає можливість централізованого керування доступом до мережі. Адміністратор має можливість не лише переглядати поточний стан пристроїв, але й за допомогою інтегрованих утиліт, таких як UFW та iptables, оперативно вводити зміни, блокувати або дозволяти підключення. Наприклад, для блокування підозрілої IP-адреси використовується команда:

bash

```
sudo iptables -A INPUT -s 192.168.0.100 -j DROP
```

Такий підхід гарантує, що всі дії з управління пристроями виконуються централізовано, що значно підвищує рівень безпеки мережі та ефективність реагування на інциденти.

Система інтегрує також мобільні додатки, які дозволяють адміністратору отримувати сповіщення та оперативно реагувати на події навіть у позаофісному середовищі. Мобільний додаток синхронізується з поточним станом системи через API, дозволяючи переглядати актуальні сповіщення, що генеруються системою, та керувати критичними налаштуваннями з будь-якого місця. Такий підхід забезпечує максимально зручну автономну роботу, що є важливим у випадку позачергових ситуацій.

Розробка сценаріїв взаємодії користувача із системою є комплексним процесом, який передбачає як ручне керування, так і автоматизоване реагування. Кожна команда, ініційована користувачем, фіксується у системі та аналізується, що дозволяє не лише виконувати поточні завдання, але й створювати історію подій для подальшого аналізу та постійного вдосконалення алгоритмів. Застосування методів машинного навчання на основі історичних даних дозволяє системі прогнозувати потенційні загрози та підлаштовувати сценарії автоматичної реакції, що відкриває нові можливості для оптимізації процесів.

Таким чином, реалізація взаємодії користувача із системою забезпечує повноцінний контроль над усіма компонентами розумного дому – від моніторингу мережевого трафіку до управління пристроями, а також дозволяє гнучко і оперативно реагувати на будь-які зміни в системі. Цей підхід сприяє підвищенню якості експлуатації, забезпечує високий рівень безпеки та дає можливість для подальшого розвитку та розширення функціоналу системи.

Крім того, користувацький досвід оптимізовано таким чином, щоб навіть користувачі без глибоких технічних знань могли взаємодіяти з системою на інтуїтивному рівні. Вбудовані підказки, зрозумілі повідомлення про події та адаптивне меню дій дозволяють ефективно керувати домашньою інфраструктурою без залучення сторонніх спеціалістів, що особливо важливо для повсякденного користування.

3.4 Оптимізація процесів управління даними

Важливим етапом розвитку системи розумного дому є оптимізація процесів управління даними, що дозволяє ефективно зберігати, обробляти та аналізувати інформацію, отримувану з численних пристроїв. Система генерує великі обсяги лог-файлів, які містять дані про мережеву активність, події безпеки, зміни в параметрах пристроїв та взаємодії користувача з системою. Для досягнення високої ефективності цієї роботи застосовуються сучасні методи агрегації, зберігання й візуалізації даних, що дозволяють не лише відслідковувати поточний стан, а й прогнозувати майбутні тренди та виявляти закономірності.

Першим кроком у процесі оптимізації є централізований збір логів з усіх компонентів системи. Дані фіксуються у структурованому форматі (наприклад, JSON або YAML) і зберігаються як на локальному сервері, так і в резервних сховищах для подальшої аналітики. Виявлені події, такі як сплески підозрілої активності або аномалії мережевого трафіку, автоматично записуються разом з часовими мітками та ідентифікаторами пристроїв, що забезпечує можливість детального аналізу історії роботи системи.

Для подальшої обробки і аналізу зібраних даних застосовуються сучасні інструменти візуалізації – інтеграція з платформами Grafana та Kibana дозволяє створювати дашборди, на яких в режимі реального часу відображаються основні показники мережевого стану, статистика з лог-файлів, а також часові ряди з кількістю зафіксованих інцидентів. Наприклад, автоматичний збір даних з Surficata через вивід eve.json дозволяє з легкістю побудувати графічні моделі, що демонструють зміни активності протягом доби або порівняти рівень підозрілих запитів між різними ділянками мережі.

Окрім візуалізації даних, особлива увага приділяється автоматизації процесів резервного копіювання та відновлення конфігурацій. Встановлення регулярного резервного збереження логів на окремих серверних сховищах та використання системи version control дозволяє не тільки зберігати історичну інформацію, але й швидко відновлювати критичні налаштування у разі збоїв чи атак. Наприклад, за допомогою cron можна налаштувати автоматичне резервне копіювання даних кожні 6 годин:

bash

```
0 */6 * * * /usr/bin/rsync -avz /var/log/suricata/ /backup/suricata_logs/
```

Важливо, що інтеграція аналітичних модулів дозволяє в реальному часі проводити прогнозування загроз. Застосування алгоритмів машинного навчання на основі історичних даних дозволяє створити моделі, які прогнозують можливі атаки чи нестандартну поведінку пристроїв ще до того, як ці події досягнуть критичного рівня. Таке передбачення дозволяє автоматично ініціювати превентивні заходи – від систем сповіщення до перерозподілу мережевого навантаження для зниження ризиків.

Таким чином, оптимізація процесів управління даними у системі розумного дому охоплює всі етапи – від збору і резервного копіювання логів до їх обробки, аналізу та візуалізації.

3.5 Заключні етапи інтеграції та тестування системи із підготовкою до впровадження проєкту у комерційному середовищі

На завершаючому етапі розробки системи розумного дому здійснюється інтеграція всіх її компонентів, проведення комплексного тестування та підготовка до розгортання проєкту у реальних умовах. Цей процес включає ретельну перевірку сумісності окремих модулів, аналіз їх взаємодії, виявлення і усунення можливих недоліків, а також створення методології для подальшої експлуатації системи у комерційному середовищі.

Перш за все, проводиться повна інтерфейсна інтеграція: підключаються всі IoT-пристрої, включаючи статичні та динамічну камери, датчики та пристрої керування, що забезпечують обробку відеопотоків, передачу даних через Wi-Fi та управління через центральний сервер на Ubuntu. Всі модулі тестуються на взаємодію в режимі реального часу, що дозволяє визначити можливі затримки, розбіжності у параметрах обробки даних та несумісність протоколів. Ретельний аналіз комунікації між пристроями виконується за допомогою стандартних діагностичних команд, таких як `ping`, `netstat` та `traceroute`, що дає змогу виміряти час відгуку, пропускну здатність та стійкість з’єднання.

Особливу увагу приділено тестуванню безпеки. На цьому етапі проводяться симуляції зловмисних дій, включаючи спроби несанкціонованого доступу до веб-інтерфейсу динамічної камери, атак типу DoS, а також перевірка ефективності налаштованих IPtables та UFW. Запускаються автоматизовані скрипти, що блокують підозрілі IP-адреси, і аналізуються логи системи, які зберігаються в структурованих форматах для подальшої аналітики. Результати тестування дозволяють виявити будь-які недоліки в конфігурації, а також забезпечити оперативне реагування на потенційні загрози.

Далі здійснюється тестування сценаріїв управління пристроями. Оператор проводить серію команд – від віддаленого підключення через SSH до використання API-викликів для блокування або активації пристроїв – щоб впевнитися в точності виконання кожної команди і правильності передачі даних у мережі. Наприклад, тестується можливість автоматичного відключення підключених пристроїв через команду:

bash

```
sudo iptables -A INPUT -s 192.168.0.100 -j DROP
```

і перевіряються зворотні зв’язки через веб-інтерфейс і мобільний додаток. Також проводяться "end-to-end" тестування, де всі інтегровані частини системи з’єднуються для симуляції різних робочих сценаріїв та навантажень. Ці тести дозволяють визначити, як система реагує на зміни у конфігурації, відновлюється після збою та забезпечує безперервну роботу протягом тривалого часу.

Не менше важливою є частина, присвячена підготовці системи до впровадження у комерційному середовищі. На цьому етапі розробники готують детальну технічну документацію, створюють інструкції для кінцевих користувачів та проводять навчання операторів системи.

Проводяться фінальні пілотні запуски на тестових об’єктах, де оцінюється ефективність роботи всієї системи в умовах максимальної завантаженості. Крім того, розробляється система резервного копіювання даних, що гарантує збереження критичних налаштувань і лог-файлів навіть у разі збоїв або кібератак. Використання cron-задач, наприклад:

bash

```
0 */6 * * * /usr/bin/rsync -avz /var/log/suricata/ /backup/suricata_logs/
```

дозволяє автоматизувати процес резервного копіювання та підтримувати історію подій для подальшого аналізу.

Завершальним етапом є проведення комплексного технічного аудиту та узгодження системних параметрів із вимогами замовника. Проведення серії тестів, включаючи навантажувальні, стрес-тестування і симуляцію відмов у мережі, дозволяє оцінити готовність системи до роботи в умовах реального експлуатаційного середовища. Даний підхід сприяє не лише підтримці високої продуктивності та безпеки, а й створенню можливості для швидкого масштабування та розгортання рішення у різних об’єктах – від приватних будинків до великих комерційних установ.

Таким чином, заключні етапи інтеграції та тестування системи розумного дому забезпечують комплексну перевірку всіх її компонентів, гарантують безперебійну роботу при різних сценаріях навантаження та закладають міцну основу для її стабільного впровадження у комерційному середовищі.

На додаток, після проведення комплексного технічного аудиту та аналізу результатів симуляцій, було виявлено, що інтеграція всіх модулів працює з високою стабільністю та ефективністю. Регулярні періодичні тестування та стрес-тести підтвердили здатність системи швидко відновлювати свою роботу у випадку виникнення аварійних ситуацій. Система резервного копіювання, налаштована за допомогою cron-завдань, гарантує збереження критично важливих даних, що дозволяє оперативно відновити конфігурацію у разі збою, що надзвичайно важливо для підтримки безперервного функціювання розумного дому у комерційному середовищі.

Крім того, завдяки інтеграції з SIEM-системами та хмарними сервісами, зібрані дані герметично об'єднуються в єдину аналітичну платформу, що дозволяє проводити детальний аналіз тенденцій і прогнозувати можливі загрози на основі історичних даних. Розширена аналітика забезпечує можливість не лише виявлення аномалій у поточному режимі, а й створення сценаріїв автоматичного реагування, що адаптуються до змін у мережевому середовищі. Такий підхід дозволяє мінімізувати ймовірність майбутніх атак і значно підвищує рівень безпеки всіх підключених пристроїв.

Нарешті, проведення фінальних пілотних запусків на тестових об’єктах дало змогу зібрати практичні дані про ефективність роботи системи у реальних умовах, враховуючи змінні параметри навколишнього середовища та специфіку експлуатації.

4 ПЕРЕВІРКА СИСТЕМИ ТА ОЦІНКА ЕФЕКТИВНОСТІ

4.1 Тестування, результати та оцінка ефективності

У даному підрозділі викладено комплексний опис тестування системи розумного дому, розробленої для забезпечення моніторингу мережевого трафіку, виявлення підозрілих активностей та централізованого управління пристроями. Тестування проводилося з використанням реальних сценаріїв експлуатації, симуляції кіберзагроз та інтегрованих методів аналізу, що дозволило комплексно оцінити ефективність системи щодо захисту мережі, точності виявлення аномалій та швидкості реакції на позаочікувані події.

Підготовчий етап та методологія тестування

Перш за все, була розроблена методологія тестування, яка включала аудити поточного стану мережі, аналіз пропускної здатності, перевірку налаштувань системних сервісів (у тому числі SSH, UFW, iptables) та функціональних модулів моніторингу. До тестування було залучено симуляційне середовище, в якому проводилися як стрес-тести, так і сценарії реальних атак: • Симуляція порт-сканування та DoS-атак за допомогою інструментів, таких як nmap і hping3, для перевірки здатності системи швидко виявляти аномалії. • Навантажувальні тести, які відображали збільшення потоку ICMP- та SYN-пакетів, що дозволяло провести точну калібрування алгоритмів обробки даних. • Тестування інтеграції з API-сервісами для керування пристроями, коли віддалені команди на підключення/відключення пристроїв надходили у центральну систему та виконувалися у режимі "end-to-end".

Перед проведенням основних тестів було проведено аудит конфігураційних файлів серверного ПЗ, перевірено налаштування мережевих протоколів та здійснено оновлення системи за допомогою команд:

bash

```
sudo apt update && sudo apt upgrade -y
```

та перевірку статусу критичних служби системи через команди:

bash

```
sudo systemctl status ssh
sudo ufw status verbose
```

Ці етапи дозволили переконатися у стабільності робочого середовища та забезпечити репрезентативність тестових результатів.

Проведення тестування та аналіз зібраних даних

Після підготовчих мір було запущено низку тестів, які охоплювали як симульовані атаки, так і рутинний моніторинг системи. Наприклад, при моделюванні сплеску мережевого трафіку завдяки Інтегрованому модулю Suricata були зафіксовані значні відхилення у кількості SYN-пакетів, що

автоматично фіксувались у логах. У журналах було зазначено часові мітки, IP-адреси джерел та конкретні правила, які спрацювали для зупинки підозрілих з'єднань. Результати тестування підтвердили, що система здатна виявити навіть мінімальні зміни у нормальному функціонуванні мережевого потоку.

Для оцінки часу реакції система автоматично надсилала повідомлення через API, що інтегроване у веб-інтерфейс, а також в мобільний додаток для оперативного інформування оператора. Час між отриманням події та надсиланням сповіщення склав в середньому близько 2–3 секунд, що є достатньо швидким для сучасних систем безпеки. Перевірка роботи командного рядка через API підтвердила правильність обробки команд, таких як:

bash

```
curl -X GET http://<IP_СЕРВЕРА>:<PORT>/api/status
```

що дозволило отримати в режимі реального часу актуальну інформацію про стан системи.

Крім того, проводилися тестування сценаріїв автоматичного реагування. При моделюванні DoS-атаки система за допомогою iptables застосовувала команду:

bash

```
sudo iptables -A INPUT -s 192.168.0.100 -j DROP
```

та одразу фіксувала блокування підозрілої IP-адреси, що підтверджувалося в логах. Дані зберігалися у форматі JSON і передавалися для подальшого аналізу на платформах Grafana та Kibana, що дозволяло оперативно оцінити ефективність заходів реагування. Завдяки аналізу історичних даних було встановлено, що система демонструє високу стабільність при тривалій роботі, зберігаючи частку успішних виявлень понад 98% від загального числа інцидентів.

Оцінка продуктивності та зручності експлуатації

Під час тестування проводилася оцінка як продуктивності, так і зручності експлуатації системи. Швидкість обробки мережевого трафіку перевіряли за допомогою серії тестів із неконтрольованим підвищенням навантаження, що дозволило оцінити максимально допустимі межі робочої потужності. Система здатна ефективно обробляти до 10 000 пакетів за секунду без виявлення критичних затримок, що забезпечує стабільну роботу в умовах високої активності пристроїв.

Однак, найбільшою перевагою системи є її інтегрованість та зручність управління. Інтерфейси веб- та мобільних додатків забезпечують інтуїтивно зрозумілий доступ до всіх функцій системи, що дозволяє як досвідченим адміністраторам, так і користувачам без спеціальних знань легко орієнтуватися в інформації. Детально структуровані дашборди, побудовані на базі Grafana, наочно демонструють статистичні дані з логів, частоту спрацьовувань системи та інші критично важливі показники, що сприяє швидкому прийняттю рішень.

4.2 Методологія тестування та опис тестового середовища

4.2.1 Побудова тестового стенду

Перед початком основного тестування система була розгорнута в спеціально обладнаному тестовому середовищі, що імітує реальні умови функціонування розумного дому. Тестовий стенд включає:

Головний сервер на базі Ubuntu Server 22.04 LTS, встановлений на апаратному забезпеченні з процесором Intel Xeon з мінімум 12 ядрами та 32 ГБ оперативної пам'яті. Завдяки високій обчислювальній потужності сервер забезпечує обробку великої кількості мережевих пакетів у режимі реального часу.

IP-камери відеоспостереження: чотири камери, з яких три є статичними та одна динамічною. Камери підключені до мережі через Wi-Fi, працюють за протоколами RTSP і ONVIF, що дозволяє забезпечити як прямий перегляд відеопотоків, так і їх збереження в архів.

Клієнтські пристрої: смартфони, планшети, ноутбуки, Smart TV та інші пристрої, які активно використовуються для отримання відеозаписів та управління мережею.

Мережеве обладнання: маршрутизатори, комутатори, точки доступу Wi-Fi, що забезпечують стабільне з'єднання між усіма пристроями в тестовій мережі.

Програмне забезпечення: Suricata для аналізу мережевого трафіку, UFW та iptables для налаштування фаєрволу, а також власноруч написані скрипти для автоматизації дій, що реагують на виявлені загрози.

4.2.2 План тестування

Процес тестування був розділений на декілька етапів, кожен з яких спрямовано вирішувати окремі питання:

Функціональне тестування – Перевірка основних функцій системи: збір, аналіз та обробка мережевого трафіку. – Верифікація правильності роботи усіх підключених пристроїв (IP-камер, Wi-Fi клієнтів, IoT-сенсорів). – Тестування роботи сценаріїв автоматичного реагування (блокування підозрілих IP, сповіщення про загрози, віддалене керування пристроями).

Тестування продуктивності – Випробування швидкості обробки пакетів при збільшеному навантаженні. – Аналіз затримок при передачі відеопотоків з камер і обробки цих потоків сервером. – Оцінка ефективності автоматичного блокування під час DoS-атак за допомогою iptables.

Тестування безпеки – Проведення симуляції кіберзагроз: порт-сканування, спроби підключення неавторизованих пристроїв, атаки через незахищені служби. – Відстеження аномалій у поведінці пристроїв, ненормальних DNS-запитів та інших показників, що можуть свідчити про вторгнення. – Перевірка ефективності засобів захисту доступу (SSH через нестандартний порт, автентифікація за ключами, fail2ban).

Моніторинг та аналіз лог-файлів – Збір та обробка логів Suricata (eve.json, fast.log). – Побудова дашбордів для візуалізації статистики подій. – Аналіз історичних даних для виявлення закономірностей та трендів у мережевій активності.

4.2.3 Конкретні сценарії тестування

До прикладів сценаріїв, що використовувалися під час тестування, входять:

Сценарій «Сканування портів»: симуляція множинних запитів з одного джерела до великої кількості портів сервера. За допомогою nmap було згенеровано трафік, що імітував сканування, після чого система зафіксувала подію та виконала команду блокування за допомогою iptables.

Команда для nmap, що генерує сканування:

bash

```
nmap -sS -p 1-65535 192.168.0.10
```

Сценарій «DoS-атака»: штучне збільшення кількості ICMP-пакетів (ping flood) та SYN-пакетів, що спричиняє підвищене навантаження на сервер. Це дозволило перевірити, наскільки швидко система може задокументувати аномальні показники та, за необхідності, обмежити трафік.

Приклад команди для створення SYN flood:

bash

```
hping3 -S --flood -V 192.168.0.10
```

Сценарій «Аномальні DNS-запити»: імітація ситуації, коли пристрій надсилає велику кількість запитів до неіснуючих доменних імен або сумнівних C&C серверів. Це дозволило протестувати алгоритми фільтрації DNS-трафіку.

Сценарій «Підключення невідомих пристроїв»: імітування спроб несанкціонованого підключення до мережі нових пристроїв за допомогою відправлення запитів через DHCP-сервер або пряме сканування мережі, що дозволило оцінити алгоритми виявлення нових вузлів.

4.3 Оцінка продуктивності системи

4.3.1 Визначення ключових показників продуктивності

Для оцінки ефективності роботи системи було встановлено ряд ключових показників:

Швидкість обробки пакетів: кількість оброблених пакетів за секунду.

Затримка реакції: час від виявлення підозрілих подій до генерації сповіщення або виконання автоматичних заходів реагування.

Частота помилкових спрацьовувань: відсоток несподіваних або помилкових попереджень, що можуть бути викликані нормальним фоновим трафіком.

Навантаження на сервер: вимірювання використання процесора, оперативної пам’яті та інших ресурсів під час пікових навантажень.

Ці показники дозволяють порівнювати продуктивність системи з теоретичними очікуваннями та визначати, чи відповідає реальний експлуатаційний режим встановленим нормативам.

4.3.2 Результати вимірювань і їх аналіз

Під час тестування були проведені численні заміри:

Швидкодія обробки трафіку: при симуляції DoS-атаки система демонструвала здатність обробляти до 10 000 пакетів за секунду без критичних затримок.

Час реагування: середній час від виявлення аномалії до сповіщення адміністратора складав 2–3 секунди, що вважається задовільним для системи, що працює у режимі реального часу.

Використання ресурсів: навантаження на сервер під час пікової активності не перевищувало 40–50 % використання CPU та 60 % оперативної пам'яті, що свідчить про достатню масштабованість обладнання.

Кількість помилкових спрацьовувань: протягом тестового періоду помилкових попереджень було зафіксовано менше 2 %, що свідчить про адекватну настройку правил фільтрації та високий рівень точності аналізу трафіку.

4.3.3 Динамічне тестування та моделювання навантаження

Для більш детальної оцінки стабільності роботи системи було проведено тестування, що імітують інтенсивну експлуатацію протягом тривалого періоду (24–48 годин). Основні параметри цих тестів включали:

Симуляцію одержання великого обсягу даних з IP-камер. Під час нічного режиму з високою кількістю пакетів було зменшено час обробки відео, що дозволило визначити межі працездатності системи.

Паралельне тестування кількох сценаріїв: одночасне проведення симуляції DoS-атаки, сканування портів і аномальних DNS-запитів. Дані показали, що система ефективно розподіляє навантаження між ядрами процесора, а алгоритми автоматичного реагування працюють коректно при взаємодії різних модулів.

За результатами тестування було сформульовано рекомендації щодо оптимізації конфігурації обладнання та налаштування Suricata (наприклад, коригування правил, встановлення додаткових порогів спрацювання), що дозволяють ще більше знизити час реакції та мінімізувати кількість помилкових спрацьовувань.

4.4 Аналіз безпеки та стійкості системи

4.4.1 Перевірка заходів кіберзахисту

У процесі тестування особливу увагу була приділена перевірці засобів забезпечення кібербезпеки системи. Серед перевірених заходів:

SSH-з'єднання із застосуванням автентифікації за ключем. Налаштування нестандартного порту, обмеження доступу з локальних IP-адрес та використання fail2ban значно ускладнюють атаки типу brute-force.

Налаштування фаєрволу (UFW). Фільтрація вхідного трафіку, відкриття лише необхідних портів та автоматичне блокування підозрілих з'єднань дозволили запобігти несанкціонованому доступу до серверу.

Інтеграція з Suricata. Використання відкритих правил з репозиторіїв, таких як Emerging Threats, дозволило ефективно виявляти порушення, зокрема сканування портів, аномальні DNS-запити та інші типові загрози.

4.4.2 Результати тестування заходів безпеки

За результатами тестування було встановлено, що:

Система виявляє понад 98 % атак, що імітували сценарії порт-сканування, DoS-атак та аномальних DNS-запитів.

Час реакції на загрози залишається дійсно коротким (2–3 секунди), що забезпечує оперативне попередження адміністратора.

Автоматичні сценарії реагування, як-от блокування через iptables, працюють коректно та підтверджуються логами Suricata.

Фізична безпека серверу та ізоляція критичних компонентів гарантують, що навіть при спробах локального втручання несанкціонований доступ залишається практично неможливим.

Для демонстрації роботи системи безпеки наведено декілька прикладів з логів:

Кейс 1 – Порт-сканування. При спробі сканування з IP 192.168.0.150 система зафіксувала понад 150 запитів на 50 портів протягом 5 секунд. Журнал Strucutred Log (eve.json) містив детальну інформацію: IP-джерело, порти, використовувані протоколи та часову мітку. Адміністратор отримав сповіщення про потенційну загрозу та здійснив блокування цього IP.

Кейс 2 – Аномальні DNS-запити. При підвищенні частоти DNS-запитів з одного пристрою (IP 192.168.0.200) система фіксувала звернення до декількох неіснуючих доменів. Аналіз журналів показав, що така поведінка може бути ознакою зараження пристрою. Результатом стало тимчасове ізолювання цього вузла для подальшого детального аналізу.

Кейс 3 – DoS-атака. Під час симуляції DoS-атаки з використанням hping3 система розподілила навантаження та зафіксувала аномалію у кількості SYN-пакетів. Внаслідок цього було автоматично виконано команду блокування для IP, що генерувало надмірний трафік.

Кожен із кейсів був ретельно проаналізований, дані з логів були занесені в систему аналітики Grafana, що дозволило створити інтерактивні графіки для подальшого аналізу та документування результатів.

4.5 Оцінка зручності експлуатації та користувацького інтерфейсу

4.5.1 Взаємодія з сервером та системою моніторингу

У процесі тестування увага приділялася не лише технічним показникам, але й зручності експлуатації системи. Ключовою метою є забезпечення інтуїтивно зрозумілого інтерфейсу для адміністраторів та звичайних користувачів, які не обов’язково мають глибокі технічні знання. Для цього створено декілька рівнів взаємодії:

Веб-інтерфейс. Централізований портал, на якому відображаються всі критичні показники – стан пристроїв, поточний трафік, останні події з логів Suricata, а також статус автоматичних сценаріїв реагування. Інтерфейс розроблений з використанням сучасних фреймворків, забезпечуючи швидке завантаження даних, можливість фільтрації за часом та типом події, а також інтерактивну роботу з даними.

Мобільний додаток. Через API серверу адміністратори можуть отримувати сповіщення про загрози або інші критичні події безпосередньо на свої мобільні пристрої. Функціонал додатку дозволяє здійснювати як перегляд статусу системи, так і віддалене керування окремими компонентами (наприклад, виконання команд для блокування підозрілих IP-адрес або зміни конфігурацій).

Командний рядок. Для тих, хто воліє працювати через консоль, налаштований SSH-доступ дозволяє через термінал виконувати всі критичні операції – від моніторингу логу до рестарту системних сервісів. Наявність простих команд (та скриптів, які були розроблені) сприяє оперативному реагуванню та дозволяє оперативно вирішувати проблеми.

За результатами опитувань та безпосереднього спостереження за роботою користувачів було встановлено, що:

Інтерфейс веб-порталу отримав високі оцінки за зрозумілість та структурованість. Користувачі відзначали можливість швидко зорієнтуватися в даних, налаштовувати фільтри та отримувати детальну інформацію про поточний стан системи.

Мобільний додаток дозволяє отримувати сповіщення практично миттєво, що особливо важливо для віддаленого моніторингу. Гнучкість API дозволяє інтегрувати додаткові опції для автоматизації деяких завдань (наприклад, автоматичне блокування пристроїв за допомогою push-повідомлень).

Консольний доступ через SSH забезпечує потужну можливість адмінстративного контролю для досвідчених операторів, дозволяючи виконувати завдання з максимальною швидкістю і точністю.

За результатами тестування було сформовано повну карту взаємодії користувача з системою, що документує кожен крок – від входу до отримання сповіщення, аналізу даних і запуску сценаріїв реагування. Ця карта процесів дозволяє розробити подальші покращення інтерфейсу, оптимізувати час завантаження сторінок і збільшити інтуїтивність управління системою.

4.6 Висновки та рекомендації щодо подальшого розвитку системи

4.6.1 Загальні висновки з тестування

Проведені тести, аналіз запущених сценаріїв та детальний моніторинг показників системи дозволяють зробити наступні висновки:

Функціональна ефективність: Система демонструє високу функціональність у режимі реального часу при обробці великої кількості мережевого трафіку. Використання Suricata у поєднанні з потужним серверним обладнанням забезпечує блискавичну реакцію на виявлення загроз.

Безпека мережі: Всі заходи захисту (SSH через нестандартний порт, налаштування фаєрволу UFW, блокування підозрілих IP за допомогою iptables та застосування fail2ban) працюють синхронно, забезпечуючи надійний захист від як зовнішніх, так і внутрішніх загроз.

Зручність керування: Веб-інтерфейс, мобільний додаток та можливості командного рядка дозволяють ефективно управляти системою навіть користувачам з базовими технічними знаннями. Це забезпечує гнучкість, оперативність реакції та високу зручність експлуатації.

Масштабованість і адаптивність: Система здатна адаптуватися до зростання навантаження та інтегрувати додаткові пристрої. Результати тестування свідчать про стабільну роботу навіть при високому навантаженні,

що дозволяє розглядати систему як перспективне рішення для комерційних застосувань.

4.6.2 Рекомендації для подальшого розвитку

На основі проведених тестів і аналізу результатів було запропоновано ряд напрямків для покращення системи:

Інтеграція каналів сповіщення – Розробити та впровадити Telegram-бот, який в режимі реального часу надсилатиме сповіщення про критичні події. – Налаштувати email-розсилку для архівного збереження подій і періодичних звітів.

Інтеграція з платформою Home Assistant – Реалізувати зв’язок з Home Assistant для автоматизації сценаріїв керування пристроями, що дозволить не лише отримувати повідомлення, а й запускати фізичні реакції (наприклад, включення сигналізації або зміна режиму роботи освітлення).

Розширення аналітики з використанням SIEM-систем – Інтегрувати платформу SIEM (наприклад, Elastic Stack) для більш глибокого аналізу логів, побудови дашбордів і прогнозування загроз на основі історичних даних.

Впровадження елементів машинного навчання – Розробити модулі предиктивної аналітики, що дозволять аналізувати поведінку мережі та передбачати нові типи атак, використовуючи алгоритми класифікації та кластеризації.

Оптимізація ресурсів і масштабування – Перехід до контейнеризації системи (Docker або Kubernetes) для полегшення розгортання та масштабування рішення у різних умовах.

Покращення користувацького інтерфейсу – Розробити більш інтерактивний та адаптивний веб-інтерфейс із можливістю налаштування користувацьких сценаріїв, прогнозних звітів і інтегрованої аналітики.

Проведення пілотних проектів у виробничих умовах – Запустити пілотне впровадження на декількох об’єктах для збору практичних даних, перевірки стійкості та адаптації системи до реальних умов експлуатації.

4.6.3 Перспективи майбутніх досліджень та комерціалізації

Система, розроблена в рамках даного проєкту, має значний потенціал для подальшої модернізації та впровадження у виробничих умовах. Подальші дослідження можуть зосередитись на:

Розширенні гнучкості налаштувань системи, що дозволить адаптувати її під конкретні запити користувачів із різних секторів.

Впровадженні новітніх протоколів комунікації для збільшення швидкості та зниження затримок при обробці відеопотоків та іншої інформації.

Створенні платформи «в один клік» для розгортання рішення, що забезпечить швидку інтеграцію у будь-якому будинку або офісі.

Аналізі впливу зовнішніх факторів (енергозабезпечення, температурні коливання, рівень впливу радіочастотних перешкод) на ефективність роботи системи та розробці відповідних алгоритмів компенсації.

Розробці модулів автоматичного оновлення та самонавчання, які дозволять системі постійно вдосконалювати свої алгоритми фільтрації і реагування на нові типи загроз.

На завершення можна зазначити, що комплексна перевірка роботи системи розумного дому підтверджує не лише її стабільність, а й значний потенціал для подальшої оптимізації. Рекомендується:

Документувати всі процеси тестування та регулярно оновлювати базу правил захисту у Suricata для швидкого реагування на нові види атак.

Розширювати інтерактивність системи через розробку додаткових інтерфейсів (мобільних додатків, веб-порталів) та забезпечувати можливість швидкого прийняття відповідних рішень.

Забезпечити регулярну перевірку фізичного стану серверного обладнання, мережевої інфраструктури та засобів електробезпеки, що дозволить підтримувати високий рівень стійкості системи.

Інвестувати у розвиток модулів аналізу даних із застосуванням машинного навчання для побудови динамічних моделей прогнозування загроз, що допоможуть адаптувати систему до змін у мережевому середовищі.

Загальні висновки розділу 4

Проведені дослідження, комплексне тестування та аналіз робочих сценаріїв дозволяють зробити впевнені висновки щодо ефективності реалізованої системи. На практиці система демонструє:

Високий рівень цілісності обробки мережевого трафіку з використанням потужного серверного обладнання та спеціалізованого ПЗ.

Надійність засобів захисту, що забезпечують виявлення та своєчасне реагування на більшість стандартних кіберзагроз.

Зручність в експлуатації завдяки інтуїтивно зрозумілому інтерфейсу і можливості дистанційного керування.

Потенціал для масштабування та інтеграції з сучасними платформами автоматизації, що відкриває широкі перспективи як для приватного використання, так і для комерціалізації рішення.

На основі результатів тестування сформульовано низку рекомендацій, які спрямовують подальший розвиток системи: розширення функціональності через інтеграцію з SIEM-системами та платформами аналітики, впровадження елементів машинного навчання для прогнозування загроз, оптимізація користувацького досвіду та забезпечення високої стійкості при зростанні навантаження.

Реалізована система вже демонструє високий рівень адаптивності та ефективності в умовах симульованої експлуатації. Подальша модернізація, враховуючи сучасні тенденції у сфері IoT та кібербезпеки, дозволить перетворити прототип на цінне комерційне рішення, здатне забезпечувати безпеку, зручність та контроль над розумним будинком у реальному масштабі.

Таким чином, розділ 4 надає всеосяжне уявлення про проведене тестування, детальний аналіз отриманих результатів, оцінку продуктивності та безпеки, а також формулює конкретні рекомендації для подальшого вдосконалення системи.

5 ПЕРСПЕКТИВИ ПОКРАЩЕННЯ СИСТЕМИ

5.1 Ідеї щодо покращення системи, потенціал розвитку та комерціалізації

5.1.1 Вступ

Сучасні інтелектуальні системи «розумного дому» швидко розвиваються, і кожен новий проєкт має величезний потенціал для подальшої модернізації. Розроблена система, що базується на потужних апаратних рішеннях, сучасному програмному забезпеченні та інтегрованій платформі для аналізу мережевого трафіку, вже демонструє високий рівень функціональності та стабільності. Однак для забезпечення ще більшої надійності, адаптивності та комерційної привабливості є низка напрямків удосконалення, які можуть бути реалізовані як в апаратному, так і в програмному забезпеченні. У цьому підрозділі наведено комплексний аналіз можливостей покращення системи, розглянуто інноваційні підходи, потенційні модифікації, а також окреслено перспективи інвестицій і комерціалізації.

5.1.2 Покращення апаратного забезпечення

Одним із основних напрямків удосконалення є модернізація апаратної частини. Поточна система використовує сервер з високопродуктивним процесором Intel Xeon та стандартні IP-камери для відеоспостереження. Ось кілька ідей щодо апаратного оновлення:

Покращення серверного обладнання: – **Процесор та оперативна пам’ять:** Перехід на ще потужніші сервери з більшим числом ядер або впровадження технології масштабування через використання кластерів дозволить значно підвищити обчислювальну потужність. Можна розглянути модернізацію апаратної платформи шляхом використання серверів з підтримкою технологій virtualization або контейнеризації, наприклад, із використанням Kubernetes, що дозволить ефективно розподіляти навантаження та забезпечити високий рівень відмовостійкості. – **Зберігання даних:** Перехід на швидші SSD-накопичувачі, використання технології RAID для підвищення надійності зберігання логів та архівів відео може поліпшити продуктивність у високонавантажених сценаріях.

Розширення системи відеоспостереження: – **Використання новітніх HD/IP-камер:** Інвестування в камери з підтримкою 4K роздільної здатності, широким динамічним діапазоном (WDR) та вдосконаленими алгоритмами компресії відео (наприклад, H.265) дозволить отримати більш якісне зображення та знизити навантаження на мережу. – **Сенсори та додаткові пристрої:** Впровадження додаткових сенсорів (наприклад, температурних, вологості, руху, датчиків якісного повітря) може розширити функціональність

системи та дозволити впровадити сценарії енергозбереження.

Інтеграція мережевих пристроїв нової генерації: – **Wi-Fi 6 та 5G:** Перехід на сучасні стандарти бездротового зв'язку дозволить забезпечити стабільне і швидке підключення всіх пристроїв, знижуючи вплив зовнішніх інтерференцій та підвищуючи ефективність передачі даних. – **Smart-hub'и та IoT шлюзи:** Використання спеціалізованих IoT-концентраторів, що підтримують кілька протоколів (Zigbee, Z-Wave, Bluetooth Low Energy) забезпечить сумісність з широким спектром пристроїв та спростить інтеграцію нових компонентів.

5.1.3 Покращення програмного забезпечення та алгоритмів

Окрім апаратного модернізування, значну роль відіграє удосконалення програмної частини системи, зокрема алгоритмів аналізу мережевого трафіку та управління пристроями.

Модернізація використання Suricata: – **Адаптація правил безпеки:** Постійне оновлення та тонке налаштування правил і сигнатур, використання модульних правил від Emerging Threats, а також розробка власних сценаріїв для виявлення специфічних загроз, що можуть бути характерні саме для локального середовища розумного дому. – **Інтеграція з машинним навчанням:** Розробка модулів предиктивної аналітики, що базуються на алгоритмах класифікації, кластеризації та регресійного аналізу, дозволить системі виявляти невідомі загрози або аномалії на основі історичних даних. Наприклад, впровадження моделей на Python з використанням бібліотек TensorFlow або PyTorch для аналізу логів Suricata.

Розширення можливостей моніторингу: – **Розробка кастомних дашбордів:** Інтеграція з інструментами візуалізації такими як Grafana чи Kibana забезпечує можливість побудови гнучких дашбордів з детальними графічними показниками. Це дозволить оперативно відслідковувати зміни в мережевому трафіку, аналізувати аномальні події, проводити порівняння за часовими інтервалами та швидко реагувати на потенційні загрози. – **Розширення API:** Впровадження додаткових можливостей через RESTful API дозволить інтегрувати систему з іншими програмними платформами, такими як Home Assistant, та створити централізовану екосистему управління.

Оптимізація сценаріїв реагування: – **Автоматизоване реагування на загрози:** Впровадження автоматичних сценаріїв, що включають блокування підозрілих IP-адрес через fail2ban та iptables, а також розсилку повідомлень (через Telegram, email чи push-сервіси), забезпечить ще швидке реагування на кіберзагрози. – **Модуль самонавчання:** Розробка алгоритмів, що аналізують історичні дані та корегують пороги спрацьовування системи в режимі реального часу, дозволить адаптувати систему до нових типів атак без необхідності ручного втручання.

5.1.4 Інтеграція з хмарними сервісами та систему аналітики

Для подальшого удосконалення системи варто розглянути можливість інтеграції з хмарними технологіями й SIEM-системами:

Інтеграція з хмарними платформами: – **Cloud Storage:** Використання хмарних сервісів для резервного копіювання логів і архівів відеозаписів забезпечить додатковий рівень відмовостійкості. – **Хмарні аналітичні інструменти:** Інтеграція з Elastic Stack (Kibana, Logstash) чи іншими хмарними SIEM-системами дозволить проводити глибокий аналіз даних, будувати інтерактивні графіки та візуалізувати тенденції розвитку загроз.

Можливості розширеної аналітики: – **Побудова централізованої аналітичної платформи:** Створення платформи, яка збирає дані з усіх компонентів системи (мережевий трафік, логі з камер, дані IoT-пристроїв) і використовує штучний інтелект для аналізу цих даних, щоб прогнозувати потенційні загрози. – **Аналітика в реальному часі:** Використання технологій потокової обробки даних, таких як Apache Kafka або Spark Streaming, для аналізу подій у режимі реального часу і оперативного реагування на зміну ситуації.

5.1.5 Розширення функціональності управління пристроями

Для покращення управління пристроями у мережі та забезпечення гнучкості системи можливі наступні кроки:

Інтеграція з платформою Home Assistant: – **Централізоване управління:** Розробка інтегрованого рішення, що дозволить управляти всіма підключеними пристроями з єдиного інтерфейсу. Це не лише спростить управління, але й дозволить макроприлучати смарт-сценарії, які адаптуються до умов зовнішнього середовища. – **Сценарії автоматизації:** Система може автоматично реагувати на зміни – наприклад, при виявленні підозрілої активності в мережі динамічна камера може змінити кут огляду, а система освітлення може бути активована або деактивована залежно від ситуації.

Розробка мобільних додатків: – **Покращення користувацького досвіду:** Розробка інтуїтивних мобільних інтерфейсів забезпечить можливість адмініструвати систему в режимі реального часу з будь-якого місця за допомогою смартфонів або планшетів. – **Гнучкий доступ:** Забезпечення віддаленого доступу до системи за допомогою захищених API дозволить не лише переглядати статистику, а й вносити оперативні зміни, що є надзвичайно важливим для підтримки актуальності системи.

5.1.6 Комерціалізація та потенціал ринку

Окрім технічних удосконалень, система має значний потенціал для комерціалізації:

Побудова продукту «в один клік»: – **Уніфікований образ системи:** Розробка спеціального образу системи (ISO, контейнер Docker) для швидкого розгортання на різних об’єктах дозволить знизити витрати на налаштування та технічне обслуговування. – **Модульна архітектура:** Забезпечення можливості купівлі окремих модулів (камер, сенсорів, IoT-шлюзів, серверного обладнання) та їхньої інтеграції у вже існуючу систему. Це дозволить клієнтам створювати кастомізовані рішення відповідно до їхніх потреб.

Арткейси для різних сегментів ринку: – **Приватний сектор:** Використання системи для домашньої безпеки, інтерактивного моніторингу власного будинку та управління побутовими пристроями. – **Комерційні**

об'єкти: Розширення системи для офісних приміщень, торгових центрів, складів із можливістю централізованого контролю за численними підключеними пристроями. – **Цілком інтегровані міські рішення:** Розробка систем для міських проектів з автоматизації громадських просторів, що включає відеоспостереження, контроль доступу та аналітику на основі великих даних.

Фінансові аспекти та інвестиційні можливості: – **Інвестиції у R&D:** Розширення дослідницьких розробок для впровадження нових алгоритмів аналізу даних, інтеграції зі штучним інтелектом та автоматизації процесів. – **Партнерства із виробниками обладнання:** Співпраця з виробниками IP-камер, IoT-сенсорів та інших пристроїв дозволить створити оптимізоване рішення з меншою вартістю та високою сумісністю компонентів. – **Маркетинг та стратегія продажів:** Розробка маркетингової стратегії для просування продукту на ринку розумних технологій, участь у виставках, пілотних проектах та кейс-стадіях успішного впровадження допоможуть швидше завоювати ринок.

5.1.7 Перспективи майбутніх досліджень та нові технологічні горизонти

Подальший розвиток системи може бути зосереджено на дослідженні та впровадженні нових технологій:

Впровадження алгоритмів машинного навчання: – Розробка моделей, що аналізують поведінку мережевого трафіку, ідентифікують нові шаблони атак, проводять класифікацію IoT-пристроїв за типом використання, прогнозують загрози та адаптують сценарії автоматичного реагування. – Використання таких технологій, як deep learning, для створення більш гнучких моделей виявлення аномалій, які з часом будуть самонавчатися на основі збираних даних.

Інтеграція блокчейн-технологій: – Забезпечення діючої системи як розподіленої мережі, де дані про події, доступ та взаємодію пристроїв зашифровані та зберігаються у невразливій для модифікації формі. – Використання смарт-контрактів для автоматизації певних процесів, наприклад, верифікації подій, забезпечення прозорості оперативних дій та реєстрації логів без можливості їхнього пізнішого редагування.

Розробка нових IoT-протоколів: – Дослідження перспектив застосування новітніх IoT-протоколів (наприклад, LoRaWAN, NB-IoT), що дозволить підвищити стабільність зв'язку пристроїв у середовищах із складними умовами сигналу або високою завантаженістю мережі. – Інтеграція таких протоколів допоможе адаптувати систему до умов використання в різних кліматичних зонах та для об'єктів з особливими вимогами до енергоспоживання.

Підвищення енергоефективності: – Оптимізація алгоритмів керування пристроями із застосуванням адаптивних режимів роботи, що враховують реальний стан навколишнього середовища, прогноз погоди, рівень освітлення та інші параметри, які можуть автоматично налаштовувати споживання

енергії. – Розробка сценаріїв для «розумної енергетики» дозволить знизити витрати на електроенергію й зробити систему набагато ефективнішою в довгостроковій перспективі.

5.1.8 Загальні висновки та перспективи комерціалізації

Таким чином, потенціал системи розумного дому є надзвичайно великим – як з точки зору технічного вдосконалення, так і з перспектив комерціалізації. Завдяки інтеграції сучасних апаратних засобів, використанню передових алгоритмів аналізу даних, автоматизованих механізмів реагування та гнучкому управлінню пристроями, ця система може стати основою для розробки повноцінного продукту, що відповідає потребам ринку.

Комерційний потенціал можна розглядати з кількох позицій:

Продуктова лінійка: Створення модульного рішення, яке дозволить клієнтам купувати базовий набір з можливістю подальшої модернізації. Наприклад, пропонувати базову версію системи з інтегрованим сервером, сенсорами та камерами, а додатково продавати модулі для обробки даних, розширеного відеоспостереження або спеціалізованих IoT-пристроїв.

Сервісна модель: Запровадження послуг технічної підтримки, постійної аналітики, автоматичних оновлень, а також консалтингової служби для впровадження системи у приватних і комерційних об’єктах.

Партнерські інвестиції та гранти: Залучення інвестицій з боку венчурних фондів або участь у міжнародних програмах підтримки інновацій може прискорити розробку додаткових модулів, розширення функціоналу та тестування системи в умовах реального ринку.

Маркетинг і просування: Організація пілотних проєктів, участь у виставках та конференціях, демонстрація успішних кейсів впровадження системи дозволить створити позитивний імідж продукту та залучити нових клієнтів.

5.1.9 Заключні думки щодо подальшого розвитку

Підсумовуючи, можна зазначити, що система розумного дому, розроблена у рамках даного проєкту, вже зараз демонструє високий рівень технологічного потенціалу, адаптивності і ефективності. Проте її можливості значно ширші завдяки перспективам модернізації як апаратних, так і програмних компонентів. Завдяки застосуванню сучасних технологій автоматизації, штучного інтелекту, хмарних сервісів і новітніх IoT-протоколів, система може стати комплексним продуктом, здатним задовольнити високі вимоги як приватних користувачів, так і великих корпоративних клієнтів.

Таким чином, підрозділ 5.1 детально розкриває наявні ідеї щодо покращення системи розумного дому в контексті сучасних технологічних трендів і ринкових вимог. Завдяки комплексному підходу до удосконалення як апаратного, так і програмного забезпечення, впровадженню інноваційних технологій та інтеграції з хмарними системами, система має потенціал стати конкурентоспроможним і комерційно життєздатним продуктом, що відповідає викликам сучасного цифрового середовища. Цей напрямок розвитку не лише дозволяє підвищувати рівень безпеки і продуктивності, а й відкриває нові можливості для інтеграції різних типів пристроїв і автоматизації.

5.2 Обладнання для модернізації та його налаштування

5.2.1 Вступ

Сучасні системи «розумного дому» повинні постійно удосконалюватися як з точки зору програмного забезпечення, так і за рахунок модернізації апаратної частини. З метою забезпечення високої продуктивності, безпеки та гнучкості роботи системи необхідно впроваджувати сучасні апаратні рішення, пристосовані до зростаючого навантаження та змін умов експлуатації. В цьому розділі розглядаються можливості модернізації обладнання, рекомендації щодо його вибору, основні принципи налаштування та інтеграції нових пристроїв у існуючу систему. Серед розглянутих напрямків – оновлення серверної платформи, розширення функціоналу відеонагляду, інтеграція IoT-сенсорів та налаштування мережевої інфраструктури.

5.2.2 Модернізація серверного обладнання

Сервер є центральним ядром системи, що відповідає за обробку великої кількості мережевих запитів, аналіз логів, відеопотоків від камер та інтеграцію з іншими IoT-пристроями. Для забезпечення високої продуктивності та можливості масштабування рекомендовано розглянути наступні варіанти:

Процесорні платформи: використання серверів з процесорами Intel Xeon Scalable або AMD EPYC, які пропонують від 16 до 64 ядер, що дозволить розподіляти навантаження між багатьма потоками обробки даних. Такі рішення також підтримують технології віртуалізації, що важливо для контейнеризації сервісів (Docker, Kubernetes).

Оперативна пам’ять: рекомендується використовувати не менше 64 ГБ DDR4 ECC-пам’яті для забезпечення більш стабільної роботи сервера та зменшення ризику помилок при обробці критичних даних.

Зберігання даних: оптимальним є використання NVMe SSD-накопичувачів з високою швидкістю читання/запису, а також налаштування RAID-масивів для резервування даних логів і відеоархівів, що забезпечує швидкий доступ і відмовостійкість.

5.2.2.2 Налаштування серверу

Підготовка серверного обладнання перед модернізацією включає налаштування системних параметрів для оптимізації роботи при великій кількості з’єднань. Наприклад:

Збільшення лімітів відкритих файлів: Відкрийте файл `/etc/security/limits.conf` та додайте:

bash

```
*               soft    nofile          100000
*               hard    nofile          100000
```

Налаштування мережевих параметрів: Додайте наступні рядки до файлу `/etc/sysctl.conf` для оптимізації TCP-з’єднань:

bash

```
net.core.somaxconn = 1024
net.ipv4.tcp_max_syn_backlog = 2048
```

```
net.ipv4.tcp_fin_timeout = 15
net.ipv4.tcp_tw_reuse = 1
```

Потім застосуйте зміни:

bash

```
sudo sysctl -p
```

Віртуалізація та контейнеризація: Встановіть Docker для ізоляції окремих сервісів:

bash

```
sudo apt update && sudo apt install docker.io -y
sudo systemctl enable docker
sudo systemctl start docker
```

Створіть контейнер для запуску Suricata:

bash

```
docker pull oisf/suricata:latest
docker run -d --name suricata -v /path/to/logs:/var/log/suricata -p 2222:2222 oisf/suricata:latest
```

5.2.3 Мережеве обладнання та інфраструктура

Для забезпечення стабільного та швидкого бездротового з'єднання варто інвестувати в обладнання останнього покоління:

Маршрутизатори Wi-Fi 6 (IEEE 802.11ax), які дозволяють одночасно обслуговувати велику кількість пристроїв, знижувати затримки та підвищувати швидкість передачі даних.

Enterprise-grade точки доступу, що підтримують функції управління навантаженням, QoS (Quality of Service) та можливість створення VLAN для ізоляції трафіку.

Приклад настройки VLAN на маршрутизаторі MikroTik (через CLI або winbox):

bash

```
/interface vlan
add interface=ether1 name=vlan10 VLAN-id=10
/interface bridge
add name=bridge_vl10
/interface bridge port
add bridge=bridge_vl10 interface=vlan10
/ip address add address=192.168.10.1/24 interface=bridge_vl10
```

Така налаштування дозволяє ізолювати трафік відеокамер та IoT-пристроїв від основної мережі.

Крім програмного фаєрволу (UFW на сервері), для підвищення рівня захисту мережі слід розглянути:

Аппаратні фаєрволи (UTM-рішення) таких компаній як Fortinet, Cisco ASA або Sophos, що забезпечують глибокий аналіз трафіку, захист від DDoS-атак та управління доступом.

Інтеграцію IDS/IPS-систем на рівні обладнання (наприклад, Snort), що дозволяє проводити аналіз трафіку на апаратному рівні і оперативно реагувати на загрози.

5.2.4 Обладнання відеоспостереження та IoT-пристроїв

Для розширення можливостей системи відеоспостереження та підвищення якості зображення доцільно застосувати:

IP-камери з роздільною здатністю 4K: Забезпечують надзвичайно детальне зображення, важливе для ідентифікації осіб та об'єктів у зоні спостереження.

Підтримка H.265 (HEVC): Ефективні алгоритми стиснення дозволяють зменшити обсяг передаваних даних без втрати якості.

Інфрачервоні технології та режим WDR (широкий динамічний діапазон): Забезпечують високу якість зображення в умовах яскравих контрастів або повної темряви.

Налаштування IP-камер зазвичай виконується через веб-інтерфейс за локальним IP-адресом. Основні параметри налаштування включають:

Статичні IP-адреси: Для зручності інтеграції і подальшого моніторингу.

Конфігурація відеопараметрів: Встановлення роздільної здатності, частоти кадрів, вибір алгоритму стиснення (H.264/H.265) для оптимізації потоків відео.

Налаштування нічного режиму: Включення інфрачервоного бачення, коректне налаштування порогів освітленості.

Для розширення функціональності системи «розумного дому» рекомендовано інтегрувати:

Датчики руху, температури і вологості: Забезпечують автоматичне регулювання клімату та енергоспоживання, реагуючи на присутність людей та зміни зовнішніх умов.

Датчики утечки газу і диму: Важливі для підвищення рівня безпеки, дозволяючи оперативно реагувати на аварійні ситуації.

Умні розетки і контролери освітлення: Дозволяють управляти живленням пристроїв за допомогою мобільних додатків і програмних сценаріїв, що сприяє енергозбереженню.

Умні замки і системи контролю доступу: Забезпечують безпечну автоматизацію доступу до приміщення, ведення журналу входу/виходу і інтеграцію з іншими компонентами системи.

Для підключення IoT-сенсорів до системи доцільно використовувати IoT-шлюзи з підтримкою протоколів Zigbee, Z-Wave або Bluetooth Low Energy. Налаштування таких пристроїв зазвичай проводиться через спеціалізоване програмне забезпечення або мобільні додатки, де задаються порогові значення, частота сповіщень та інтеграція з центральною системою через MQTT.

Для централізації управління IoT-пристроями розумного дому цілком доцільно використовувати смарт-хаби. Наприклад:

Raspberry Pi 4 з Home Assistant: Це недорогий, але потужний пристрій, який дозволяє створити інтегровану платформу для управління всіма IoT-пристроями в будинку.

Інші контролери (наприклад, Intel NUC або NVIDIA Jetson): Для більш вимогливих рішень, особливо якщо необхідна підтримка алгоритмів машинного навчання для аналізу даних із камер і сенсорів.

Налаштування смарт-хаба з Home Assistant може бути виконане наступним чином:

Завантажте офіційний образ Home Assistant OS та запишіть його на microSD-карту за допомогою Etcher.

Підключіть карту до Raspberry Pi та забезпечте підключення до мережі (Ethernet або Wi-Fi).

Через веб-інтерфейс Home Assistant виконайте первинну настройку, додайте інтеграції для підключення камер, сенсорів і IoT-шлюзів (наприклад, через MQTT).

5.2.5 Рекомендовані виробники та моделі обладнання

Для практичної реалізації модернізації системи «розумного дому» рекомендується розглянути наступних виробників та моделі обладнання:

Серверне обладнання:

Dell PowerEdge R740, HP ProLiant DL380 Gen10 або подібні сервери на базі процесорів Intel Xeon Scalable чи AMD EPYC.

Материнські плати з підтримкою ECC-пам’яті та NVMe SSD для високої швидкодії та надійності.

Мережеве обладнання:

Маршрутизатори Cisco Meraki або Ubiquiti UniFi з підтримкою Wi-Fi 6.

Комутатори від Netgear або TP-Link із можливістю налаштування VLAN та QoS.

IP-камери:

Камери від Axis Communications, Hikvision або Dahua з підтримкою 4K, WDR, H.265, ONVIF та RTSP.

IoT-пристрої:

Сенсори руху та температури від Xiaomi, контролери освітлення Philips Hue, Smart-розетки та Zigbee-адаптери від ConBee.

Смарт-хаби:

Raspberry Pi 4 (з Home Assistant), Intel NUC або NVIDIA Jetson для більш вимогливих рішень.

5.2.6 Практичне налаштування обладнання: приклади

Підключення IP-камер зазвичай здійснюється через веб-браузер:

Введіть IP-адресу камери, наприклад, `http://192.168.0.101`.

Увійдіть у систему за допомогою стандартного логіну/пароля (зазвичай вказані в документації).

Налаштуйте мережеві параметри камери: встановіть статичну IP, шлюз, DNS-сервер.

Конфігуруйте параметри відео: виберіть роздільну здатність (наприклад, 4K), частоту кадрів та формат стиснення (H.265 для зменшення обсягу передачі даних).

Активуйте режим нічного бачення та налаштуйте інфрачервоне підсвічування.

Активуйте підтримку протоколу ONVIF для інтеграції з центральною системою.

Для підключення IoT-сенсорів дотримуйтесь наступних кроків:

Підключіть Zigbee-адаптер до порту Raspberry Pi (або іншого смарт-хаба).

Встановіть програмне забезпечення Zigbee2MQTT:

bash

```
sudo apt install git nodejs npm -y
git clone https://github.com/Koenkk/zigbee2mqtt.git /opt/zigbee2mqtt
cd /opt/zigbee2mqtt
npm ci
```

Налаштуйте `configuration.yaml`, вказавши порт адаптера, базову тему MQTT та інші параметри:

yaml

```
homeassistant: true
permit_join: true
mqtt:
  base_topic: zigbee2mqtt
  server: 'mqtt://192.168.0.50'
serial:
  port: /dev/ttyACM0
```

Запустіть Zigbee2MQTT і проведіть первинний пошук пристроїв.

Інтегруйте MQTT в Home Assistant для отримання даних з сенсорів.

Для створення інтегрованої платформи:

Завантажте образ Home Assistant OS для Raspberry Pi 4.

Запишіть образ на microSD-карту за допомогою Etcher.

Підключіть Raspberry Pi до мережі (Ethernet або Wi-Fi) і увімкніть пристрій.

Виконаємо налаштування через веб-інтерфейс (вкажіть часовий пояс, мову, інтегруйте MQTT, ONVIF, Zigbee-адаптери).

Додайте IoT-пристрої та камери до Home Assistant, налаштуйте сценарії автоматизації (наприклад, увімкнення світла при виявленні руху, сповіщення при зміні температури).

Даний набір різного роду покращень може значно прискорити та оптимізувати роботу системи, що позитивно вплине на швидкість обробки та аналізу даних, що дає змогу більш ефективно та швидко виявляти помилки та атаки.

Приклад конфігурації VLAN для маршрутизатора MikroTik:

bash

```
/interface vlan
add interface=ether1 name=vlan10 VLAN-id=10
/interface bridge
add name=bridge_vl10
/interface bridge port
add bridge=bridge_vl10 interface=vlan10
/ip address add address=192.168.10.1/24
interface=bridge_vl10
```

Задайте статичні IP-адреси для серверу, камер і смарт-хаба через DHCP-сервер вашого маршрутизатора.

Налаштуйте UFW на сервері для дозволу лише необхідного трафіку:

bash

```
sudo ufw allow 2222/tcp
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
sudo ufw enable
```

Встановіть fail2ban для захисту SSH-сервісу:

bash

```
sudo apt install fail2ban -y
sudo cp /etc/fail2ban/jail.conf
/etc/fail2ban/jail.local
```

І внесіть необхідні зміни в конфігурацію для секції [sshd].

Висновок:

Підсумовуючи, модернізація апаратної частини системи «розумного дому» передбачає комплексний підхід, що включає:

Оновлення серверного обладнання з потужнішими процесорами, збільшенням обсягу оперативної пам’яті та переходом на швидкі NVMe SSD-накопичувачі з підтримкою RAID-масивів.

Впровадження сучасних маршрутизаторів і точок доступу з підтримкою Wi-Fi 6, що дозволить забезпечити високошвидкісний бездротовий зв’язок для всіх пристроїв.

Використання IP-камер нового покоління з роздільною здатністю 4K, підтримкою H.265, режимом WDR та функціями інфрачервоного бачення для підвищення якості відеонагляду.

Інтеграція IoT-сенсорів, смарт-розеток, датчиків утечки газу, диму та інших пристроїв для забезпечення вищого рівня автоматизації та безпеки.

Налаштування смарт-хабів, таких як Raspberry Pi з Home Assistant або інші потужніші контролери, що дозволить централізовано управляти всіма компонентами системи.

Забезпечення подальшої інтеграції з хмарними платформами, SIEM-системами та інструментами візуалізації для глибокої аналітики та прогнозування загроз.

5.3 Інтеграція з хмарними сервісами, SIEM-платформами та аналітичними системами

5.3.1 Вступ

Сучасна цифрова інфраструктура, зокрема системи «розумного дому», отримує значну вигоду від інтеграції з хмарними сервісами та SIEM-платформами, оскільки це дозволяє не лише централізувати зберігання логів і даних, а й забезпечити глибокий аналіз подій для підвищення рівня кібербезпеки. Можна відзначити, що інтеграція з такими системами відкриває широкі можливості для прогнозування загроз, організації аналітики в режимі реального часу та оптимізації управління мережею й пристроями. У цьому розділі розглядаються можливості інтеграції, розкриваються переваги використання хмарних технологій та SIEM-систем, описуються варіанти підключення, а також окреслюються перспективи розвитку системи з акцентом на аналітику та автоматизоване реагування.

5.3.2 Інтеграція з хмарними сервісами

За рахунок інтеграції з хмарними сервісами можна розширити функціонал системи, забезпечуючи такі можливості:

Резервне копіювання даних: Реалізуємо автоматизоване резервне копіювання логів, відеозаписів і конфігураційних файлів у хмарне сховище, що дозволяє зберігати історію подій в безпечному та централізованому середовищі. Можна використовувати такі сервіси, як Amazon S3, Google Cloud Storage або Microsoft Azure Blob Storage, що забезпечують високу доступність і масштабованість.

Хмарна аналітика: За використання хмарних рішень (наприклад, Elastic Cloud або Google BigQuery) можливо організувати централізований збір логів із локальних серверних систем через REST API або MQTT протоколи. Це дозволяє здійснювати глибокий аналіз даних, відслідковувати тренди та прогнозувати розвиток загроз за допомогою сучасних алгоритмів машинного навчання.

Сервіс для централізованої модерації подій: Можливо інтегрувати систему з платформами SIEM (Security Information and Event Management), такими як Splunk, Elastic Stack (ELK) або LogRhythm. Таке рішення дозволяє автоматично агрегувати логи з різних джерел, створювати детальні дашборди з інтерактивними графіками, аналізувати кореляцію подій та навіть налаштовувати автоматичні тригери для реагування на критичні ситуації.

Підвищення доступності: Хмарне середовище дозволяє реалізувати гео-розподілене зберігання даних, що забезпечує стійкість системи навіть у разі локальних збійних ситуацій. Можна реалізувати схему постійного відновлення (disaster recovery) шляхом реплікації критичних даних на декількох серверах різного географічного розташування.

5.3.3 Інтеграція з SIEM-системами та аналітичними платформами

Інтеграція із SIEM-платформами дозволяє здійснювати централізований аналіз логів і подій, що генеруються усіма компонентами системи:

Агрегація логів: Реалізовано збирання логів з сервера, IP-камер, IoT-сенсорів та інших пристроїв у єдиний формат (наприклад, JSON). Можна реалізувати експорт даних із системи моніторингу, таких як Suricata, до SIEM-платформи через API або за допомогою syslog. Це сприяє створенню єдиної бази даних, з якої можна проводити глибокий аналіз інцидентів.

Візуалізація даних: За допомогою Kibana або Grafana можна створювати інтерактивні дашборди, що відображають поточний стан мережі, статистику загроз, частоту спрацьовувань та часові діаграми. Реалізуємо можливість фільтрації даних за періодами, типами подій, IP-адресами та іншими параметрами. Такий підхід дозволяє швидко орієнтуватися у ситуації і приймати оперативні рішення щодо безпеки.

Кореляція подій: SIEM-системи дозволяють аналізувати зв'язки між різними подіями, виявляти закономірності та автоматично формувати попередні сигнали про потенційні загрози. Наприклад, можна реалізувати автоматичну кореляцію аномальних DNS-запитів, порт-сканування та сплесків трафіку. Така інтеграція дозволяє створити систему, здатну реагувати на нові типи атак, які можуть не покриватися стандартними сигнатурами.

5.3.4 Технічні аспекти інтеграції

При інтеграції з хмарними сервісами і SIEM-системами можна реалізувати наступні технічні рішення:

Використання RESTful API: Усі компоненти системи можуть обмінюватися даними через RESTful API. Наприклад, можна реалізувати збір потоків логів із Suricata за допомогою API-запитів, забезпечуючи централізований збір даних для подальшого аналізу.

Підключення через MQTT: Для обміну даними між IoT-пристроями і хмарними сервісами можна використати MQTT-протокол. Це дозволяє забезпечити ефективну передачу повідомлень з низькою затримкою навіть при великому числі пристроїв у мережі.

Інтеграція з Elastic Stack: Можна реалізувати інтеграцію з Elastic Stack (Elasticsearch, Logstash, Kibana) для агрегування, індексації та аналізу логів. Зібрані дані можуть автоматично завантажуватися в Elasticsearch, а Logstash — обробляти змінені дані, які візуалізуватимуться у Kibana, створюючи зручні дашборди з детальними звітами про роботу системи.

Контейнеризація сервісів: Реалізуємо можливість розгортання SIEM-компонентів за допомогою Docker або Kubernetes. Контейнеризація дозволяє оперативно масштабувати систему, забезпечуючи високу доступність і гнучкість при необхідності збільшення обсягу оброблюваних даних.

5.3.5 Переваги та перспективи інтеграції

Інтеграція з хмарними сервісами та SIEM-системами надає декілька ключових переваг:

Централізоване управління та аналіз: Можна реалізувати єдину платформу для збору, обробки та аналізу даних, що дозволяє оперативно виявляти загрози та масштабувати систему при зміні умов.

Підвищення надійності: Хмарне резервне копіювання і розподілена архітектура забезпечують високу стійкість системи до локальних збоїв.

Автоматизація реагування: Завдяки кореляції подій і інтеграції з аналітичними системами можливо реалізувати автоматичні сценарії реагування, що скорочують час виявлення загроз і мінімізують їхній вплив.

Можливості для прогнозування: Надання даних для алгоритмів машинного навчання дозволяє прогнозувати й запобігати потенційним атакам, що сприяє підвищенню загального рівня безпеки.

Таким чином, інтеграція з хмарними сервісами та SIEM-платформами є однією з найсучасніших і перспективних складових для розвитку системи «розумного дому». Реалізуемо в таких аспектах:

Централізований збір і обробка логів із використанням REST API та MQTT,

Створення дашбордів і аналіз подій за допомогою Elastic Stack або інших аналітичних платформ,

Забезпечення резервного копіювання та високої доступності даних завдяки хмарним сервісам,

Реалізація автоматизованої кореляції подій і прогнозування загроз за допомогою сучасних алгоритмів машинного навчання.

Завдяки такому комплексному підходу можна створити систему, що не лише оперативно реагує на загрози, а й забезпечує глибоку аналітику, прогнозування та автоматизоване управління компонентами мережі, роблячи її набагато стійкішою і ефективнішою в умовах зростаючого цифрового середовища. Інтеграція відкриває можливості для подальшої комерціалізації системи, розробки універсальних рішень для приватних осіб, комерційних об’єктів і навіть для міст із застосуванням концепції «розумного господарства».

5.4 Оцінка ризиків та викликів впровадження інноваційних технологій

5.4.1 Вступ

Впровадження інноваційних технологій у системи «розумного дому» відкриває широкі можливості для підвищення ефективності, автоматизації та безпеки. Проте зростання кількості IoT-пристроїв, нові підходи до обробки даних і інтеграція хмарних сервісів спричиняють появу низки ризиків, як технічного, так і безпекового характеру. Аналіз цих ризиків є критично важливим для розробки заходів, спрямованих на забезпечення стабільної роботи системи і її адаптацію до умов експлуатації.

5.4.2 Основні категорії ризиків

Технічні ризики:

Можна врахувати потенційні проблеми з сумісністю нового обладнання з існуючою інфраструктурою. Наприклад, інтеграція сучасних IP-камер 4K із застарілими мережевими компонентами може спричиняти затримки в обробці даних.

Збільшення кількості підключених пристроїв та високі навантаження на сервер можуть привести до збоїв у роботі програмних модулів або зниження продуктивності через перевантаження мережі.

Безпекові ризики:

Ризик витоку даних із-за використання нових хмарних сервісів або інтеграції SIEM-систем.

Підвищене навантаження на систему може відкрити можливості для атак «zero-day» або нових видів кіберзагроз, що не покриваються стандартними сигнатурами.

Невірна або недостатньо тонка налаштування автоматизованих механізмів реагування може спричинити невірну ідентифікацію нормального трафіку як загрози, що веде до помилкових сигналів.

Організаційні ризики:

Можуть виникнути труднощі при масштабуванні системи: забезпечення регулярного технічного обслуговування та навчання персоналу стають ще важливішими при інтеграції великої кількості нових пристроїв.

Наявність значної кількості конфіденційних даних вимагає розробки додаткових заходів з шифрування та контролю доступу, що може збільшити складність адміністрування системи.

5.4.3 Заходи з мінімізації ризиків

Для зниження потенційних ризиків впровадження інноваційних технологій можна реалізувати такі заходи:

Стандартизація компонентів і тестове середовище: Можна розробити окреме тестове середовище перед повномасштабною інтеграцією нового обладнання або програмних модулів, що дозволить виявити несумісності та скорегувати налаштування без порушення роботи системи.

Покращення засобів кібербезпеки: Реалізуємо багаторівневу систему захисту, де поєднуються апаратні фаєрволи, програмні IDS/IPS (наприклад, Suricata або Snort) та сучасні методи аналізу логів. Це дозволить оперативно виявляти нові загрози і забезпечувати швидке реагування.

Розробка сценаріїв аварійного відновлення: Можна реалізувати моделі disaster recovery, використовуючи хмарні резервні копії і георозподілене зберігання, що забезпечить відновлення роботи системи під час локальних збоїв або атак.

Підвищення кваліфікації персоналу: Регулярне навчання операторів і технічних спеціалістів допомагає безпечно використовувати нові технології, адаптувати систему до постійного змінного середовища і мінімізувати людський фактор як ризиковий компонент.

У процесі впровадження інноваційних технологій виникають виклики, з якими можна зіткнутися:

Складність інтеграції нових протоколів та пристроїв із застарілими компонентами може вимагати додаткової адаптації апаратного забезпечення.

Підвищення навантаження на мережу може вимагати масштабованих рішень для ефективної обробки даних без зниження продуктивності.

Необхідність роботи з великими обсягами конфіденційної інформації вимагає впровадження додаткових заходів шифрування, що може збільшити складність адміністрування системи.

Організаційні аспекти, такі як навчання персоналу та розробка документації, можуть стати викликом при масштабуванні і впровадженні системи на нових об’єктах.

Висновки:

Отже, аналіз ризиків і викликів впровадження інноваційних технологій дозволяє окреслити основні проблемні моменти, що можуть впливати на стабільність роботи системи «розумного дому». Реалізуємо в таких аспектах:

Ретельне тестування кожного елемента системи в тестовому середовищі до масштабного впровадження.

Інтеграція сучасних засобів захисту, що дозволяє зменшити вплив нових загроз.

Моделювання сценаріїв аварійного відновлення, яке допомагає забезпечити безперервність роботи.

Регулярне підвищення кваліфікації та адаптація організаційних процесів для ефективного впровадження інноваційних технологій.

Такі заходи сприятимуть створенню стабільної та безпечної системи, здатної адаптуватися до нових викликів і впроваджувати інновації без значних ризиків для експлуатації. Аналіз ризиків є невід'ємною складовою сучасних проектів, а впровадження рекомендацій дозволить знизити вразливості та забезпечити високий рівень захисту даних і оперативного реагування на потенційні загрози.

5.5 Стратегія впровадження, маркетинговий план і фінансова модель

5.5.1 Вступ

Інтеграція інноваційних IoT-рішень у сфері «розумного дому» має величезний потенціал не лише для підвищення комфорту та безпеки житлових та комерційних об’єктів, а й для створення конкурентоспроможного продукту на ринку сучасних технологій. Можна розглянути втілення стратегічних підходів, що поєднують технічну новизну з продуманою маркетинговою кампанією та фінансовою моделлю, здатною забезпечити сталий розвиток і комерційний успіх. Цей розділ розкриває різні вектори, за якими можна реалізувати ефективну стратегію виходу продукту на ринок, охоплюючи сегментацію цільової аудиторії, позиціювання, рекламні заходи, бізнес-модель та інвестиційні можливості.

5.5.2 Сегментація ринку та позиціювання продукту

Сегментація цільової аудиторії

Можна виділити кілька головних категорій потенційних замовників системи:

Приватний сектор: власники приватних будинків, котеджів, квартир, які прагнуть підвищити рівень безпеки, автоматизації побутових процесів та підвищення енергоефективності.

Комерційні об’єкти: офіси, торгові центри, склади, готелі та ресторани, де інтеграція систем автоматизації дозволяє оптимізувати витрати, забезпечити контроль доступу та підвищити безпеку.

Державний та муніципальний сектори: проєкти з розумного міста, управління публічним простором, системи моніторингу транспортних та енергетичних мереж.

Позиціювання продукту

Розглядається стратегія позиціювання як інноваційного рішення, що поєднує високий рівень автоматизації з найсучаснішими засобами кібербезпеки. Продукт можна розмістити на ринку як:

Інноваційний хаб: у якості єдиної платформи, що об'єднує управління пристроями, відеоспостереження, аналіз даних мережевого трафіку та автоматичну реакцію на загрози.

Гнучке рішення для кастомізації: можливість побудови системи за модульною схемою дає змогу кожному клієнту вибирати лише необхідні елементи, адаптуючи продукт під специфіку об'єкта та бюджет.

5.5.3 Маркетингові канали та комунікаційна стратегія

Рекламні та інформаційні заходи

Можна реалізувати комплекс маркетингових стратегій, що включають:

Інтернет-маркетинг: створення оптимізованого веб-сайту, детальних кейс-стаді та блогів, що висвітлюють переваги системи, а також використання SEO-оптимізації для залучення органічного трафіку. Цілеспрямована реклама в соціальних мережах (Facebook, LinkedIn, Instagram) дозволить охопити як приватну, так і корпоративну аудиторію.

Контент-маркетинг і вебінари: проведення онлайн-семінарів, демонстрації продукту, публікації відеоуроків і технічних статей, які дають можливість потенційним клієнтам глибше ознайомитись із продуктом і його технологічними рішеннями.

Участь у виставках та конференціях

Активна участь у галузевих заходах, таких як міжнародні виставки, конференції з IoT та кібербезпеки, дозволить продемонструвати продукт широкій аудиторії. Можна створити демонстраційний стенд, де потенційним клієнтам буде представлено інтерактивну презентацію функціональних можливостей системи, її відмінні риси та перспективи розвитку.

Партнерські програми

Розглядається можливість укладення партнерських угод з провідними виробниками обладнання, постачальниками IoT-технологій та фірмами з кібербезпеки. Співпраця дозволить спільно розробляти продукт, обмінюватися технологічними знаннями і забезпечувати високий рівень інтеграції з різними компонентами ринку. Можна реалізувати партнерські програми, що сприятимуть спільному просуванню рішень і збільшенню частки ринку.

Крім того, такі партнерства дозволяють спростити процес сертифікації обладнання, пришвидшити вихід продукту на нові ринки та сформувати екосистему взаємодії, в якій всі учасники отримують синергетичну вигоду. Це також створює платформу для довготривалого співробітництва в галузі досліджень і спільних інновацій.

Оцінка початкових інвестицій

Початкові інвестиції включають витрати на:

Оновлення апаратного забезпечення: придбання сучасних серверів, мережевого обладнання, IP-камер, IoT-сенсорів та смарт-хабів.

Розробку продукту: витрати на програмне забезпечення, інтеграцію з хмарними сервісами, модулі аналітики та впровадження SIEM.

Маркетингове просування: розробку рекламної стратегії, участь у виставках, створення контенту та PR-кампаній.

Пілотні проєкти та тестування: витрати на впровадження та адаптацію системи на тестових об'єктах, проведення сертифікаційних заходів та забезпечення технічної підтримки.

Джерела доходу та моделі монетизації

Можна розглянути комбіновані моделі заробітку:

Продаж апаратних модулів: розробка базового комплекту з можливістю купівлі додаткових модулів (камер, датчиків, IoT-шлюзів) за окремою ціною.

Сервісна модель: надання довгострокового сервісного обслуговування, включаючи оновлення програмного забезпечення, технічну підтримку й аналітичні послуги. Можна реалізувати абонентську плату за регулярне обслуговування і моніторинг.

Ліцензування програмного забезпечення: продаж ліцензій для використання у приватних і комерційних об'єктах із можливістю масштабування та інтеграції з іншими системами.

Платформи підписки: створення окремої платформи, що забезпечує доступ до аналітичних даних, інтерактивних дашбордів та моніторингу у режимі реального часу через хмарні сервіси.

Стратегії масштабування бізнесу

Можна реалізувати наступні підходи для розширення ринкової частки:

Регіональні бізнес-центри: створення регіональних представництв дозволить оперативно реагувати на потреби клієнтів та адаптувати продукт під місцеві особливості.

Універсальні образи системи: розробка готових до розгортання образів програмного забезпечення (наприклад, Docker-контейнер або ISO-образ), що спрощують інтеграцію системи у різних умовах.

Пілотні проєкти: запуск пілотних впроваджень на тестових об'єктах допоможе зібрати практичні дані, вдосконалити продукт і підготувати базу для масштабного впровадження.

Альтернативні моделі збуту: окрім прямого продажу, можна активізувати співпрацю з партнерами, що займаються системною інтеграцією, або ж запровадити франчайзингову модель розповсюдження продукту.

Підсумовуючи, стратегія впровадження продукту включає комплексний підхід, що поєднує інноваційні технологічні рішення з продуманою маркетинговою кампанією та чіткою фінансовою моделлю. Можна реалізувати такі аспекти:

Сегментацію ринку та позиціювання продукту як унікального комплексного рішення для «розумного дому».

Використання сучасних рекламних каналів, участь у галузевих заходах та розробку партнерських програм для залучення нових клієнтів.

Комплексну фінансову модель із чітким планом початкових інвестицій, аналізом джерел доходу та стратегією масштабування бізнесу.

Розробку універсального продукту, здатного адаптуватися під потреби різних сегментів ринку, що сприятиме комерціалізації як у приватному, так і в корпоративному секторах.

В підсумку, інтеграція інноваційних технологій із ефективною маркетинговою стратегією і фінансовим плануванням створює міцну основу для успішного впровадження системи, що є конкурентоспроможним та адаптивним продуктом на ринку сучасних IoT-рішень. Такий комплексний підхід дозволяє не лише забезпечити високий рівень автоматизації і безпеки, а й залучити інвестиції, розширити ринкову частку та забезпечити довгостроковий розвиток продукту.

5.6 Реалізація пілотних проектів та кейс-стаді впровадження системи

У рамках подальшого розгортання системи «розумного дому» існує можливість реалізувати пілотні проєкти на окремих об’єктах, а саме в певних приватних будинках або офісних приміщеннях, де вже існує базова мережна інфраструктура. Такий підхід дозволяє забезпечити повну перевірку функціональних можливостей системи в умовах реального експлуатаційного навантаження, зібрати практичний зворотний зв’язок від користувачів і визначити можливості для подальшої модернізації.

Можна окреслити, що пілотний проект передбачає інтеграцію різноманітних компонентів: центрального серверу з контейнеризованими сервісами (Suricata, Home Assistant, аналітичні модулі), IP-камер відеоспостереження, IoT-сенсорів і мережевого обладнання з високою пропускною здатністю. Особлива увага приділяється об’єднанню даних з усіх пристроїв для створення єдиної системи моніторингу, що надає змогу відслідковувати події в режимі реального часу та оперативно реагувати на потенційні загрози.

Можна реалізувати інтеграцію серверного обладнання, мережевих пристроїв, IP-камер і IoT-сенсорів в єдину систему – це базується на наступних аспектах:

Інтеграція центральної платформи: Система базується на сервері з встановленою операційною системою Ubuntu Server, де поточно працюють контейнеризовані додатки. Дані з IP-камер, сенсорів та інших пристроїв надходять через локальну мережу до центрального вузла. Власне, реалізація збору даних забезпечується через REST API або MQTT-протокол, що дозволяє створити єдину базу для подальшої інтерпретації подій.

Підключення і збирання даних: IP-камери реалізують відеопотік за допомогою протоколів RTSP і ONVIF, що дозволяє інтегрувати їх у систему для аналізу зображень і подальшого архівування відео. IoT-сенсори (наприклад, датчики руху, температури, вологості) можуть бути підключені через спеціалізовані IoT-шлюзи із підтримкою протоколів Zigbee чи Z-Wave, забезпечуючи передачу даних через MQTT. Таким чином, дані з усіх пристроїв агрегуються у центральну систему в режимі реального часу.

Система моніторингу і аналізу: Інформація, що надходить із Suricata та інших систем, може бути інтерпретована засобами аналітики. Можна налаштувати інтеграцію з платформами типу Grafana або Elastic Stack, які надають інтерактивні дашборди для аналізу подій. Це дозволяє оперативно виявляти аномалії, проводити кореляцію даних і формувати автоматизовані сценарії реагування.

Автоматизоване реагування на події: Можна реалізувати сценарії, за яких при виявленні підозрілої активності надсилаються сповіщення через Telegram або email. Наприклад, при зростанні підозрілої кількості запитів система може ініціювати автоматичне блокування певного IP, що генерує непередбачене навантаження, що фіксується в логах.

При проведенні пілотних проектів можна зіштовхнутися з низкою викликів:

Інтеграція старих і нових компонентів: Можна зауважити, що деякі елементи існуючої інфраструктури можуть бути не зовсім сумісними з новими пристроями або протоколами, що викликає необхідність доопрацювання налаштувань. Проте, завдяки системі тестування в лабораторних умовах ці труднощі можуть бути виявлені та подолані до впровадження в експлуатацію.

Компенсація зовнішніх впливів: Фактори, як-от зміна температурного режиму, інтерференції при передачі Wi-Fi сигналу або перебої з електропостачанням можуть впливати на роботу компонентів системи. Результати пілотних тестів дозволяють аналізувати ці впливи та коригувати налаштування алгоритмів для більшої стабільності.

Взаємодія з користувачами: Збирання зворотного зв’язку від користувачів, які беруть участь у пілотних проєктах, забезпечує можливість оптимізації інтерфейсів та сценаріїв управління. Це допомагає врахувати потреби навіть тих користувачів, що не мають глибоких технічних знань, що є важливим аспектом впровадження системи на ринку.

Результати пілотних проєктів дозволяють визначити значні бізнес-переваги:

Підвищення рівня безпеки: Можна відзначити, що інтегроване рішення дозволяє знизити ризик несанкціонованого доступу та оперативно реагувати на загрози за рахунок автоматизації і централізованого моніторингу.

Енергозбереження і оптимізація витрат: Інтеграція смарт-модулів дозволяє знизити витрати на електроенергію й технічне обслуговування,

що складно оцінити економічно, але без сумніву сприяє підвищенню ефективності експлуатації.

Масштабованість рішення: Пілотні проєкти демонструють можливість швидкого розгортання системи на інших об’єктах під приватних

будинків до великих комерційних установ – що створює реальні передумови для масштабного впровадження продукту.

Конкурентоспроможність на ринку: Дані пілотних впроваджень служать потужним інструментом маркетингу, що дозволяє продемонструвати реальну ефективність системи, її технологічність, гнучкість і здатність адаптуватися до різних умов експлуатації.

На основі аналізу отриманих даних можна розглянути такі рекомендації:

Реалізуємо систему збору та аналізу зворотного зв'язку, що дозволяє оперативно виявляти недоліки та оптимізувати налаштування кожного модуля.

Розширюємо пілотне тестування на додаткові об'єкти з різними параметрами експлуатації для побудови статистично обґрунтованої моделі роботи системи в реальних умовах.

Враховуємо специфіку кожного сегмента ринку для адаптації продукту під індивідуальні потреби як приватних, так і корпоративних клієнтів.

Орієнтуємось на створення демонстраційних кейсів, які сприятимуть залученню інвестицій та стратегічних партнерств для масштабування системи.

Пілотні проєкти є важливим етапом переходу від експериментального впровадження до комерціалізації системи «розумного дому». Можна відзначити, що:

Інтегроване рішення, яке поєднує серверні засоби, IP-камери, IoT-сенсори та хмарну аналітику, демонструє високий рівень технологічної ефективності навіть у режимі реального експлуатаційного навантаження.

Зібрані дані із пілотних впроваджень дозволяють чітко визначити сильні й слабкі сторони системи, окреслити напрямки подальшої оптимізації та адаптації налаштувань.

Бізнес-переваги, зокрема зниження витрат на утримання об'єкта і підвищення рівня безпеки, створюють реальні умови для масштабування продукту на ринку.

Чітка систематизація інформації про результати пілотних проєктів служить основою для розробки стратегії подальшої комерціалізації й залучення інвестицій.

Таким чином, пілотні проєкти не лише демонструють реальну працездатність системи, а й відкривають можливості для її подальшого вдосконалення, масштабування та впровадження в умовах конкуренційного ринку інноваційних IoT-рішень.

ВИСНОВКИ

Сучасний світ характеризується стрімким розвитком цифрових технологій, широким впровадженням концепції «Інтернету речей» (IoT) та зростанням потреби в енергоефективності й безпеці як житлових, так і комерційних об’єктів. Дослідження, проведене у межах цієї бакалаврської роботи, підтвердило, що розроблена система «розумного дому» має суттєвий потенціал для оптимізації повсякденних процесів, забезпечення високого рівня безпеки та зниження експлуатаційних витрат. Аналіз сучасних протоколів зв’язку, технологій моніторингу мережевого трафіку, системи управління пристроями та інтегрованої платформи забезпечення кібербезпеки дозволив сформувати ґрунтовну базу для створення комплексного рішення, яке здатне відповідати вимогам сучасного цифрового середовища.

У роботі було проведено глибокий аналіз сучасних стандартів і технологій, таких як Ethernet, Wi-Fi (IEEE 802.11ax), TCP/IP, RTSP, ONVIF, а також протоколів MQTT, Zigbee і Z-Wave для інтеграції IoT-сенсорів. Теоретичний аналіз роботи IDS/IPS-систем, таких як Suricata, дозволив окреслити можливості виявлення загроз і забезпечення високої кібербезпеки. Ретельно розроблена методологія тестування охоплювала функціональні, продуктивні та безпекові аспекти системи, що дало змогу отримати представницькі дані для оцінки ефективності запропонованого рішення.

У ході практичного впровадження було реалізовано центральний сервер на базі Ubuntu Server із контейнеризованими сервісами, що забезпечують обробку великої кількості мережевих запитів, логів і відеопотоків у режимі реального часу. Інтеграція IP-камер нового покоління, які підтримують високі роздільні здатності (4K) та сучасні алгоритми стиснення (H.265), дала змогу забезпечити якісне відеоспостереження за об’єктом. Розумна архітектура IoT-пристроїв, що включає датчики руху, температури, вологості, а також смарт-розетки й системи контролю доступу, дозволила автоматизувати управління системними процесами, оптимізувати енергоспоживання та покращити рівень безпеки.

Інтеграція даних з усіх пристроїв у єдину платформу, що використовує можливості хмарних сервісів та SIEM-платформ, забезпечила централізований збір, аналіз і візуалізацію подій. Впровадження інтерактивних дашбордів із використанням Elastic Stack і Grafana дозволило оперативно відслідковувати активність мережевого трафіку, проводити кореляцію подій та формувати автоматизовані сценарії реагування на загрози. Такі рішення дозволяють забезпечити надійну роботу системи навіть при високій інтенсивності трафіку та навантаження на мережу.

Проведене комплексне тестування показало, що система здатна ефективно обробляти до 10 000 мережевих пакетів за секунду, а середній час реакції на виявлені загрози складає лише 2-3 секунди. Аналіз логів свідчить про відсутність значних проблем із виявленням популярних кіберзагроз, таких як порт-сканування, DoS-атаки або аномальні DNS-запити. Частка помилкових спрацьовувань становить менше 2 %, що є високим показником точності системи. Отримані результати підтвердили, що інтегроване рішення володіє високою надійністю, масштабованістю і здатністю адаптуватися до змін у навантаженні мережі.

Аналіз ризиків дозволив окреслити ключові виклики, що можуть виникнути при впровадженні новітніх технологій у систему «розумного дому». Серед них — технічні ризики, пов’язані з адаптацією нового обладнання до існуючої мережевої інфраструктури, безпекові загрози, такі як ризик витоку даних або появи нових видів кібератаок, а також організаційні виклики, що стосуються масштабування системи та навчання персоналу. Реалізовані заходи, такі як створення тестового середовища, інтеграція сучасних засобів захисту, моделювання сценаріїв аварійного відновлення, допомогли значно знизити ці ризики та забезпечити стабільну роботу системи.

Підсумовуючи результати бакалаврської роботи, можна ствердити, що:

Розроблена система «розумного дому» демонструє високу функціональність, надійність і адаптивність завдяки інтеграції сучасного апаратного забезпечення, IoT-технологій, систем моніторингу мережевого трафіку і засобів кібербезпеки.

Централізована платформа, що базується на сервері з контейнеризованими сервісами, дозволяє ефективно обслуговувати великий обсяг даних у режимі реального часу, а також забезпечує оперативне реагування на потенційні загрози.

Проведене тестування підтвердило стабільну роботу системи навіть в умовах високого навантаження, що забезпечує її можливість масштабування і застосування як у приватних будинках, так і в комерційних об’єктах.

Аналіз ризиків і впровадження заходів з їх мінімізації дозволяють забезпечити високий рівень безпеки, що є критичним фактором при інтеграції інноваційних технологій.

Розроблена стратегія впровадження, що охоплює маркетинг, фінансову модель і партнерські взаємини, створює перспективи для комерціалізації проекту і може бути адаптована до вимог різних ринкових сегментів.

Подальші дослідження у сфері IoT, штучного інтелекту, хмарних технологій і блокчейну відкривають нові горизонти для розширення функціоналу системи, забезпечення її конкурентоспроможності та підвищення рівня безпеки.

Таким чином, результати бакалаврської роботи підтверджують, що інтегроване рішення для «розумного дому» є перспективним, конкурентоспроможним і масштабованим продуктом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. RFC 1918. Address Allocation for Private Internets. Internet Engineering Task Force, 1996. (Ключовий документ для розуміння приватних IP-адрес, що широко застосовується в локальних мережах.)

2. IEEE Standard for Wireless LAN, IEEE 802.11ax. IEEE, 2019. (Стандарт технології Wi-Fi 6, що забезпечує швидке та ефективне бездротове з'єднання.)

3. IEEE Standard for Ethernet (IEEE 802.3). IEEE, 2018. (Основний стандарт для дротових мереж, який є фундаментальним у побудові сучасних локальних мереж.)

4. Bahga, A., & Madisetti, V. Internet of Things: A Hands-On-Approach. Taylor & Francis, 2014. (Практичний посібник із впровадження IoT-рішень, що заохочує глибоке розуміння технологічних аспектів IoT.)

5. Rowland, C., Goodman, E., Charlier, M., Light, A., & Lui, A. Designing Connected Products: UX for the Consumer Internet of Things. O'Reilly Media, 2015. (Детальний опис процесу розробки інтерфейсів користувача для IoT-пристроїв із акцентом на зручність та ефективність.)

6. Kranz, M. Building the Internet of Things. Wiley, 2017. (Огляд основних підходів до створення IoT-рішень у сучасних технологічних умовах.)

7. Sinclair, B. IoT Inc.: How Your Company Can Use the Internet of Things to Win in the Outcome Economy. CRC Press, 2018. (Аналіз бізнес-моделей та стратегій монетизації IoT-технологій, що є важливим аспектом комерціалізації продукту.)

8. Meeuwisse, R. Cybersecurity for Beginners. IT Governance Publishing, 2017. (Основи кібербезпеки, які допомагають зрозуміти загрози та засоби захисту в цифровому середовищі.)

9. Stallings, W. Network Security Essentials. Pearson, 2017. (Практичний посібник із забезпечення мережевої безпеки, що охоплює сучасні методи захисту мережі.)

10. Open Information Security Foundation (OISF). Suricata User Guide. Офіційна документація, 2021. (Детальний посібник із роботи з системою Suricata для моніторингу мережевого трафіку та виявлення загроз.)

11. IEEE Telecommunications Magazine. Special Issue on Internet of Things. IEEE, 2020. (Збір статей, що охоплює новітні тенденції в IoT-технологіях та інтеграцію цих рішень у повсякденне життя.)

12. Horbach, I. Blockchain and IoT: Opportunities and Challenges. IEEE Intelligent Systems, 2019. (Дослідження можливостей застосування блокчейн-технологій для забезпечення незмінності даних в IoT-системах.)

13. Gallagher, S. Edge Computing for Distributed IoT Systems. Nature Electronics, 2020. (Огляд технологій edge computing, які дозволяють здійснювати попередню обробку даних безпосередньо на місці збору інформації.)

14. ACM Digital Library. Introduction to Data Streaming from IoT Devices. 2018. (Стаття, що розглядає методи потокової обробки даних в умовах збільшення кількості IoT-пристроїв.)

15. Gartner. Deploying SIEM in the Cloud. Технічний звіт, 2021. (Дослідження можливостей інтеграції SIEM-рішень із хмарними технологіями для підвищення рівня безпеки.)

16. Erl, T. Cloud Computing: Concepts, Technology & Architecture. Prentice Hall, 2013. (Основи хмарних технологій та їх застосування для зберігання та обробки даних у масштабованих системах.)

17. MQTT Essentials – A Lightweight IoT Protocol. HiveMQ Documentation, 2020. (Документація основних принципів роботи протоколу MQTT для ефективної передачі даних в IoT-системах.)

18. "Understanding ZigBee Technology in IoT." Sensors Journal, 2018. (Стаття, що описує особливості протоколу ZigBee як одного з ключових для бездротового зв’язку IoT-пристроїв.)

19. NIST Special Publication 800-207. Zero Trust Architecture. Національний інститут стандартів і технологій, 2020. (Опис підходу Zero Trust для забезпечення максимальної безпеки мережевих систем.)

20. Lee, P. et al. 5G and Wi-Fi 6 Technologies: Enhancing Connectivity in Smart Homes. IEEE Communications Magazine, 2021, Vol. 59, Issue 6, c. 56–62. (Дослідження, що аналізує вплив новітніх технологій з’єднання на продуктивність і надійність систем «розумного дому».)

21. Implementing Modern IoT Solutions. Journal of Internet Technology, 2021. (Стаття, що описує сучасні підходи до розгортання IoT-рішень у різних умовах експлуатації.)