ВСТУП

Швидкий розвиток технології впливає на всі сфери сучасного світу, трансформуючи його до невпізнання. Не стала винятком і людська оселя, яка із кожним днем все більше комп'ютеризується для автоматизації рутинних задач і створення комфортних умов життя. Але розумні будинки — це не тільки комфорт і енергоефективність, а й покращені системи безпеки[1].

На ринку представлено багато видів систем автоматизації і охорони в усіх цінових категоріях, від простої сигналізації до розумних роботів, але, зазвичай, ці системи продаються як «чорний ящик» і не дають змоги користувачу налаштовувати і розширювати їх згідно своїх бажань.

В цій роботі розглядаються технології за допомогою яких можна створити енергоефективну і легко розширювану бездротову систему спостереження за навколишнім середовищем розумного дому і пропонується модель такої системи.

1. Концепції, огляд технологій, постановка задачі

В сучасному світі все більше багатофункціональних розумних додатків, через розвиток в сферах мереж, обчислень і інформаційних технологій, стають частинами нашого життя. Широкого розповсюдження набули системи спостереження. Вони використовуються для забезпечення безпеки на вулицях, банках, супермаркетах, для моніторингу потенційно небезпечних або недоступних для людини середовищ (наприклад, жерл вулканів або океанських глибин) .

Комп'ютери і мережі давно стали обов'язковими частинами життя людини, все більше мережевих додатків стають поселяються в наших оселях. Хоча домашні системи спостереження встановлені у невеликої кількості людей, їх кількість зростає, ринок систем охорони значно виріс у 2016-2017 роках [2], пропоновані продукти отримують все більше функцій. Якщо раніше такі системи обмежувалися сигналізацією при вторгненні (для відлякування злодія) і виявленням диму та пожежі (для автоматичного виклику пожежників), то тепер вони здатні вимірювати температуру, помічати витоки газу і т.д. Вони роблять завдання керування домом простішим, охорону більш надійною і дають змогу власнику слідкувати, що відбувається всередині або поблизу дому, коли він у від'їзді.

Домашня система спостереження може складатися із відеокамер, терміналів, сенсорів, виконавчих механізмів, серверів. Більш загально, така система може бути використана для моніторингу та контролю приладів. Зазвичай, дані від сенсорів передаються по мережі на сервер, на якому може відбуватися аналіз даних, їх збереження, прийняття рішень і відправка команд іншим пристроям. Все частіше такі системи приєднуються до Інтернету через мережевий екран. Користувач може отримувати дані із серверу (для чого часто будуютьсь клієнтські додатки), або віддавати йому команди для управління сенсорами та пристроями. В

результаті, користувач може моніторити і контролювати свій будинок через інтернет або інші IP мережі.

В цій роботі пропонується модель системи спостереження як одного із компонентів розумного дому, яку можна підключити до існуючого рішення.

Створення «Інтелектуальних будівель» або «Розумних домів» продовжує набирати популярність у зв'язку з появою все нових доступних і простих в установці модулів для їх побудови. Спочатку, цей термін застосовувався для складних інженерних систем автоматизації, заснованих кабельно-дротовому з'єднанні. Але з появою концепції Інтернету речей (Internet of Things, IoT) «розумні будинки» стали використовувати бездротові інтерфейси зв'язку між компонентами, а також підключення до мережі Інтернет для дистанційного керування. Для того щоб спроектувати компонент систем даного типу, здатний до моніторингу та віддаленого контролю, необхідно зрозуміти основні принципи концепції «Інтернету речей» і особливості архітектури «Інтелектуальних будівель».

1.1 Інтернет речей

Що таке Інтернет речей, з яких рівнів він складається і які технології використовує? Огляд концепції, її гідності і проблеми розвитку.

1.1.1 Концепція. Визначення

Термін вперше був сформульований в 1999 році Кевіном Ештоном(Англ. Kevin Ashton), працівником дослідницької групи в компаніїProcter & Gamble. Він запропонував запровадити радіочастотну ідентифікацію – RFID-мітки або маркери (Radio Frequency IDentification), для відстеження переміщення товарів компанії.

Зміст концепції Інтернету речей можна сформулювати наступним чином: для збільшення ступеня комфорту життя людей і надання складних комплексних послуг необхідно створення глобальної інфраструктури, що складається з безлічі речей (віртуальних і фізичних), які з'єднані між собою

за коштами існуючих,що розвиваються і функціонально сумісних технологій інформаційної комунікації.

Фізичні речі в даній концепції - це речі реального фізичного світу (датчики і різні пристрої), а віртуальні – речі інформаційного світу (наприклад, віртуальні гроші, і все, що матеріальну ціну, але не має фізичного носія). Кожна з таких речей може бути ідентифікована або інтегрована в мережу.

Якщо подивитися з практичної точки зору, то концепція Інтернету речей спрямована на автоматизацію діяльності в різних сферах діяльності, виключення з них людини, і, як наслідок, підвищення ефективності економічних і суспільних процесів.

Засновник європейської ради по «Інтернету речей» Роб Ван Краненбург (бельг. Rob van Kranenburg) в своїх роботах пропонує цікаву модель Інтернету речей у вигляді «чотиришарового пирога».

Перший шар включає в себе ідентифікацію об'єктів, наприклад, за допомогою датчиків або RFID-маркерів. На цьому етапі кожна Інтернет-річ отримує засіб зв'язку з навколишнім світом і унікальні дані.

Другий шар - обслуговування споживача або сервіс. тут об'єкти об'єднуються в мережі для виконання певної функції в рамках поставленого завдання. Найпоширенішими прикладами є системи моніторингу навколишнього середовища за допомогою бездротових сенсорних мереж і, звичайно, «Розумні будинки».

Третій шар заснований на тенденції урбанізації міського життя, так звані «Розумні міста», які мають на увазі дослідження і збір інформації на конкретній території (кварталі, районі тощо) і надання всієї необхідної інформації її мешканцям.

Четвертий і найвищий рівень - це сенсорна планета, коли всі існуючі мережі об'єднуються в глобальну інформаційну інфраструктуру.

Іншими словами, Інтернет речей - це мережа мереж.

1.1.2 Архітектура і використовувані технології

Архітектуру Інтернету речей можна, можливо розділити на чотири функціональних рівня (рис. 1), розглянемо кожен з них детальніше.

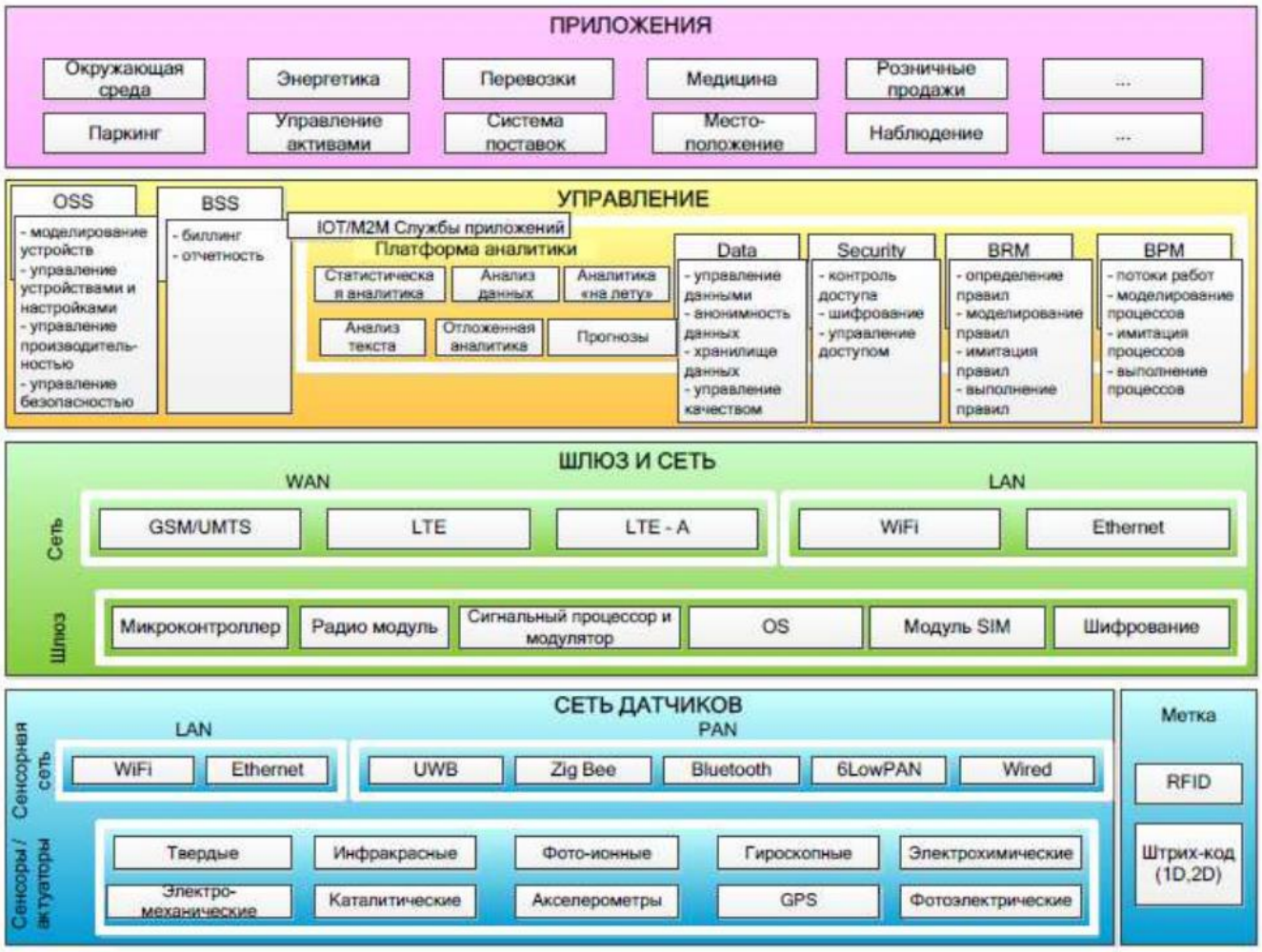

Рисунок 1 – Архітектура IoT. Поділ на функціональні рівні

Самим нижнім в структурі Інтернету речей, але в той же час і самим важливим, є рівень сенсорів. Якщо зіставити з моделлю Роба ванн Краненбурга, то він є першим шаром «Пирога».Грунтується цей рівень на модулях, до яких підключаються датчики і сенсори, а також інших об'єктах, що забезпечують збір інформації, наприклад, на RFID-мітках згадуваних раніше або штрихкодах. Такі об'єкти можуть інтегруватися один в одного і в інші фізичні об'єкти, і навіть в тіло людини.

Багато досліджень в області сенсорів проводить Інститут інженерів електротехніки та електроніки - IEEE (англ. Institute of Electrical and Electronics Engineers). На даний момент анонсований стандарт обміну

інформацією IEEE 802.15.102, що дозволяє передавати інформацію в малопотужній бездротовій мережі в безпосередній близькості до людського тілу без перешкод.

Для передачі інформації всередині домашніх або офісних мереж використовуються менш чутливі і більш енергоємні стандарти обміну, найбільш відомими з яких є Ethernet, Wi-fi і Zig Bee.

Велика частина датчиків неінформативна сама по собі, але, об'єднуючись в мережеві структури, вони несуть значний потік корисної інформації. Для об'єднання і передачі інформації в світ більшості датчиків потрібна наявність шлюзу або агрегатора сенсорів. Залежно від завдання об'єднання об'єктів і роду самих об'єктів, можливе використання одного з нижчеописаних типів мереж.

1) Бездротові сенсорні мережі (WSN, Wireless Sensor Network) - самоорганізовувані мережі датчиків і пристроїв. Як правило, пристрої мережі з'єднані радіоканалом, тому цей тип мереж відрізняється низьким енергоспоживанням, малим радіусом покриття і низькою швидкістю передачі. Радіус покриття коригується ретрансляцією повідомлень (MultiHop Networking або Ad Hoc мережі). Основним стандартом передачі є 6LoWPAN (англ. IPv6 over Low power Wireless Personal Area Networks), який дозволяє підключати сенсорні пристрої до широко поширених IP мереж.

2) Мережі ультра широкосмугового бездротового зв'язку на малих відстанях (UWB, Ultra-Wide Band) -використовуються для під'єднання периферійних пристроїв в мережах малого радіусу охоплення, наприклад,принтерів або мультимедійних систем в межах будинку. Характеризуються високою швидкістю передачі на малих відстанях.

3) Персональні мережі (PAN, Personal Area Network) — мережі,створювані «навколо» людей, об'єднують персональні комп'ютери, телефони і інші пристрої. У мережах даного типу використовуються

специфікації мережевих протоколів верхнього рівня, такі як ZigBee і Bluetooth.

4) Локальні обчислювальні мережі (LAN, Local Area Network) - Ethernet і Wi-Fi; даний тип мереж на сьогоднішній момент відомий більшості людей, так як інтернет міцно увійшов в сучаснесуспільство.

5) Глобальні бездротові мережі (WAN, Wide Area Network) - мережі, що забезпечують зв'язок пристроїв з серверами / додатками безпосередньо, якщо не потрібне підключення до агрегатору. У категорію глобальних бездротових мереж входять GSM, GPRS і LTE.

Підтримка сервісів для обслуговування вимагає IoT забезпечити суміщення великої кількості мереж з різними протоколами доступу і технологіями передачі даних. Причому конфігурація таких мереж може бути різноманітною. Другий рівень - рівень шлюзів і мереж якраз і передбачає об'єднання мереж різних типів в єдину мережеву інфраструктуру.

Об'єднані мережі вимагають особливої відповідності встановленим стандартам якості передачі інформації: затримки не повинні перевищувати допустимих норм, пропускна здатність і безпека передачі даних повинні так само відповідати стандартам. Користувачі повинні мати спільний та незалежний доступ до ресурсів без втрати продуктивності.

Наступний рівень - сервісний. Забезпечує управління бізнес-правилами і бізнес-процесами (BRM, Business Rule Management і BPM, Business Process Management відповідно). дозволяє автоматизувати операції, проведені над інформацією - збереження та аналіз, забезпечує підтримку операційної і бізнес діяльності (OSS / BSS, Operation Support System / Business Support System).

Самий верхній рівень - рівень додатків. Додатки діляться на «горизонтальні», застосовні для різних сфер діяльності і «вертикальні», створювані під певний напрям діяльності.

1.1.3 Переваги і недоліки концепції Інтернету речей

Переваги розвитку технологій Інтернету речей випливають з практичного застосування концепції: це автоматизація процесів в різних сферах діяльності, і, як наслідок, підвищення їх економічної ефективності. Інтернет речей покликаний зробити наше існування комфортнішим, а виробництво більш вигідним. Навряд чи хтось не мріє про автоматично винесене сміття і підігрітий до часу приходу додому з роботи чай або свіжозварену каву зранку.

Але це лише мала частина можливостей Інтернету речей в сфері особистого користування. Для роботи в офісах колосальну користь може принести контроль клімату в приміщенні, адже комфортне робоче середовище покращує самопочуття, підвищує працездатність і навіть настрій. А повідомлення про незакриті після робочого дня вхідні двері може вберегти від неприємностей. Автоматизація на виробництві так само допоможе уникнути непередбачених ситуацій, що особливо важливо на небезпечних хімічних і атомних підприємствах. Постійний контроль робочої зони і повідомлення при перевищенні параметрами встановлених норм може допомогти уникнути катастрофи.

Інтернет речей розвивається стрімко, але і без труднощів не обходиться. На сьогоднішній день є кілька причин уповільнення в розвитку настільки популярнї концепції: дефіцит IPv4 адрес, зменшення енергоспоживання датчиків і відсутність загальноприйнятих стандартів.

- Дефіцит адрес IPv4:

Кожен новий датчик потребує унікального IP-адресу. Адреси IPv4 закінчилися ще в лютому 2010 року. Отже, постає питання про перехід до протоколу нової версії з розширеним кількістю адрес - IPv6. Крім більшої кількості адрес, IPv6 спрощує управління мережами, так як в ньому існує функція авто-конфігурації адрес, а так само підключення по даному протоколу є більш безпечним, ніж підключення по IPv4.

- Енергоспоживання датчиків:

Енергопостачання датчиків - дуже важливе питання, тому що реалізація основної ідеї концепції Інтернету речей вимагає їх автономності. Неможливо забезпечити батарейками величезну кількість модулів без шкоди для навколишнього середовища. Необхідний інший підхід. датчики повинні отримувати енергію з навколишнього середовища або виробляти її самостійно. Найпростіший спосіб отримання енергії — сонячні батареї, але він не придатний для всіх видів датчиків, лише для тих, що розташовуються близько до джерел світла. Великий крок у розвитку був зроблений вченими Американського хімічного товариства в 2010 році. Анонсовано наногенератор - гнучкий чіп, що виробляє енергію з людських рухів. Безсумнівно, вчені розроблятимуть все нові і нові способи отримання енергії.

- Стандарти:

У галузі стандартизації були досягнуті значні результати за останні кілька років, але проблеми безпеки, захисту особистої інформації і встановлення єдиної архітектури рішень як і раніше актуальні. Уже згадувана раніше міжнародна асоціація IEEE (Інститут інженерів електротехніки та електроніки) - одна з небагатьох організацій, що сприяють розвитку єдиних стандартів. Поточним рішенням є стандартизована передача пакетів IPv6 в різних видах мереж.

Починаючи з 2012 року, Європейська комісія по питаннях інформаційного суспільства проводить консультації по темі регулювання ринку пристроїв, що підключаються до приватних бездротових мереж. Така стурбованість викликана тим, що пристроями Інтернету речей збирається, зберігається і передається інформація особистого характеру, яку зловмисники можуть використовувати проти власників. Єврокомісія намагається знайти оптимальне рішення, що поєднує захист особистих даних і зручність використання модулів і їх взаємну сумісність.

Над створенням універсальних специфікацій і відповідної сертифікації в сфері «розумної» електроніки на даний момент працюють кілька організацій, в тому числі альянс Open Connectivity Foundation (OCF), що включає в себе Intel, Samsung Electronics і Dell.

Одним з рішень проблеми безпеки є апаратна підтримка напівпровідниковими компонентами протоколу TLS (Transport Layer Security - безпека транспортного рівня). даний протокол аналогічний криптографічному протоколу SSL (Sockets Layer — рівень захищених сокетів), так як використовує симетричне шифрування і асиметричну криптографію, але захищає дані на більш низькому рівні.

1.2 Інтелектуальні будівлі

Концепція «Розумного дому», з чого складаються системи автоматизації будівель і чим спричинена популярність напрямку зараз.

1.2.1 Визначення і архітектура “Розумних будівель”

Автоматизація будівель почала з'являтися ще в 60-70-х роках минулого століття, тоді і було сформульовано поняття «розумний будинок». спочатку воно формулювалося як «будинок для ефективного використання робочого простору», але на сьогоднішній день його сенс набагато ширше.

«Розумний будинок» для сучасної людини - не просто система раціонального використання робочого простору, це інтелектуальна система, яка об'єднує в собі як інженерні комунікації та системи безпеки, так і інформаційні системи будівлі. Такі об'єднані рішення покликані підвищити комфортність приміщень і забезпечити їх безпеку. У багатьох випадках приводом для установки систем розумного будинку є бажання підвищити ступінь комфорту за рахунок автоматизації рутинних дій.

Реалізація розумного будинку ділиться на дві частини: апаратну і програмну. На рис. 1.2 представлена одна з можливих і найбільш часто використовуваних схем апаратного забезпечення розумного будинку.

Апаратна частина, як правило, складається з контролера, модулів розширення і кінцевого обладнання.

Контролером може виступати ПК, планшет, смартфон, на які встановлюється програмне забезпечення для управління системами розумного будинку всередині домашньої (робочої) мережі або через мережу Інтернет.

Модулями або платами розширення називають спеціальні пристрої з підключеними датчиками різного типу і керованими частинами системи.

В категорію кінцевого обладнання входять датчики для відстеження різних параметрів середовища і стану пристроїв, які необхідно регулювати.

Програмне забезпечення може бути реалізовано багатьма способами: від звичайного пульта управління до складного синхронізованого комплексу програмного забезпечення, що встановлюється на будь-яку кількість гаджетів і ПК власника інтелектуальної будівлі і повністю автоматичних систем, що включають в себе елементи інтелектуалізації.

1.2.2 Дистанційне керування “Розумним домом”

Розвиток бездротових інтерфейсів зв'язку та розширення концепції Інтернету речей призвело до виходу систем розумних будинків за межі приміщень і будівель, в яких вони встановлені. Взаємодія автоматизованих комплексів з мережею Інтернет дала можливість управляти ними в режимі віддаленого доступу.

Дистанційне керування має ряд переваг перед управлінням виключно автоматичним і через системи, що працюють в межах установленного радіусу. Перш за все, це підвищення рівня безпеки і комфорту.

Основна перевага — підвищення комфорту використання простору будинку або офісу, що і є основною ідеєю для створення розумного будинку. При наявності функції віддаленого управління користувач може включити, вимкнути або налаштувати потрібні йому пристрої (освітлення,

побутові прилади та інші системи), де б він не перебував. Наприклад, підігріти чай перед приходом додому з роботи або заздалегідь включити опалення, якщо за показаннями датчиків в приміщенні некомфортна температура.

Але головною перевагою варто вважати підвищення рівня безпеки. При відсутності людей в приміщенні можуть відбутися ситуації, що загрожують схоронності майна і самої будівлі. Для запобігання подібних інцидентів можливе підключення камер для спостереження за обстановкою в приміщенні або віддалений моніторинг з допомогою аналізу інформації, що надходить від різних датчиків, які використовуються в системах безпеки (датчики вогню, датчики відкриття / закриття дверей і т. д.). В тому числі, автоматичне відключення електроприладів та світла допоможе не тільки заощадити споживання електроенергії, а й зменшити ризик самозаймання електропроводки в порожньому приміщенні;

Система дистанційного керування в більшості випадків проста: користувач, з використанням гаджетів або ПК, відсилає команди системі через веб-додаток або зі сторінки веб-сайту, система аналізує отриману команду і за допомогою контролера виконує вказану дію.

Так як дистанційна робота з датчиками, камерами і іншим обладнанням передбачає зберігання, обробку і аналіз великої кількості інформації, і зручний доступ до результатів декількома користувачами, доцільне застосування хмарних технологій. При такому підході в системі розумного будинку з'являється хмарний сервіс, який дозволяє позбавити користувача турбот щодо обслуговування серверної частини системи, за допомогою якої відбувається управління всією системою.

Для підключення хмари існує два варіанти. Перший - використання хмари в якості контролера. Всі пристрої підключаються безпосередньо до хмари і управляються з неї безпосередньо. Керуюча частина системи може

бути повністю винесена за межі будівлі. Другий варіант - збір пристроїв на контролерах і підключення їх до хмари. В цьому випадку хмара буде керувати діями контролерів, передаючи інформацію між кількома модулями. контролер розміщується всередині будівлі, але все програмне забезпечення винесено на сервіс.

Обидва варіанти передбачають винесення аналізуючої частини системи в хмару, що дозволяє знизити вимоги до контролера, головна відмінність в тому, що в першому випадку управління пристроями ведеться автономно один від одного, а в другому - через загальний контролер.

Багато сучасних модулі працюють по власних протоколах передачі даних і, взаємодіють з Інтернет-сервісами тільки через свої API, що створює складності обміну інформацією між пристроями безпосередньо, а також заважає розширенню системи розумного будинку.

1.3 Системи безпеки розумних будинків

Потреба забезпечення безпеки змушує людей шукати все нових способів і технологій для захисту своєї власності. Багато систем пропонує контроль над внутрішнім та/або зовнішнім середовищем дому. Об'єднання різних елементів безпеки будівлі укупі з іншими технічним обладнанням в єдину автоматизовану мережу дає, мабуть, самий відчутний ефект від вкладених в «розумний дім» коштів.

Безпека в розумному будинку: 5 аспектів

Мова йде не тільки про захист від непрошених гостей, але і про запобігання аварійних ситуацій. Система безпеки покликана забезпечити особисту безпеку мешканців приватного будинку, співробітників підприємства, злагоджене функціонування всіх служб житлового,

офісного, виробничого або торгового будівлі.

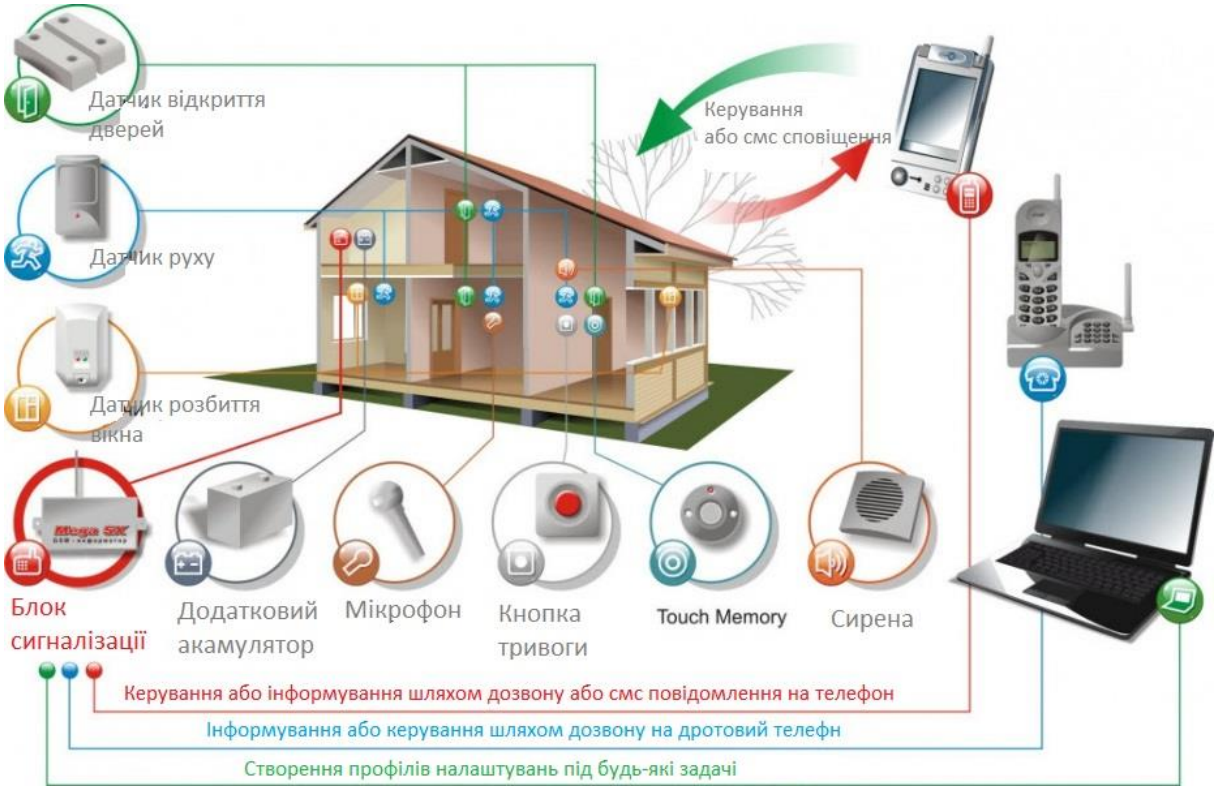

рисунок 1.4. системи безпеки розумних будинків

Охоронна сигналізація

Всі можливі шляхи попадання в дім (вікна, двері, терито навколишньої ділянки) оснащуються сенсорам проникнення. Всередині кімнат дому розміщують пристрої, що реагують на переміщення людей. При цьому домашні тварини можуть переміщатися по будинку вільно. На випадок, якщо зловмисники все ж проникли в будинок, обдуривши господарів, встановлюються приховані тривожні кнопки, їх можна носити і в кишені.

Контроль здійснюється зонально, реакція на зміну ситуації може бути різною: повідомлення на пульт охорони поліції або іншого відомства, SMS господареві або його довіреним особам. Наприклад, про несанкціоноване проникнення в будинок повідомлення буде отримувати служба охорони, а про відкриття сейфа або навіть про те, що хтось надмірно цікавий входив в робочий кабінет - тільки господар будинку.

Охоронна сигналізація може працювати в декількох режимах. Наприклад, в нічний час під охорону може здаватися тільки периметр території та приміщення першого поверху. Які системи безпеки можуть входити до складу «розумного будинку»?

Контроль доступу

Всі двері, ворота, шлагбауми можуть бути оснащені пристроями доступу, як кодовими, так і зчитують інформацію з карт доступу, радіочіпи, або розраховані на отримання біометричних даних. Персоналізація засобів доступу дозволить мати точну інформацію про пересування по будівлі домочадців або працівників. Не всім співробітникам, відвідувачам або домашнім працівникам буде довірено право входу в деякі приміщення. До систем контролю доступу можна віднести і захист вікон: ролети і механічні віконниці. Їх закриттям і відкриттям можна управляти за допомогою заданого алгоритму або вручну.

Відеоспостереження

Домофон; камери, розташовані поза і всередині будівлі, через контролер підключаються до телекомунікаційних пристроїв. Вони дають можливість спостерігати за тим, що відбувається всередині поза будівлею з будь-якого телевізора або комп'ютера, встановленого в будинку. Або дистанційно, з пульта охорони, комп'ютера або екрану смартфона.

Камери можуть бути як видимими, так і зовсім непомітними. Події реєструються на відео, записи належний час зберігаються на сервері.

Пожежна і аварійна сигналізація, безпека інженерних систем

Аварійні інженерні мережі припускають наявність датчиків вогню, диму, витоку газу і води. У разі небезпеки тривожне сповіщення надходить в ДСНС або диспетчерську житлових або відомчих служб. При відповідному сигналі буде припинено надходження в будівлю газу,

перекриті водопровідні вентилі. Включиться система автоматичного пожежогасіння, якщо вона є в будівлі.

Енергетична безпека забезпечується системою енергозабезпечення. У разі припинення подачі електроенергії протягом декількох секунд вводиться в дію автоматичний резерв, включається автономна генераторна установка, побудована на базі двигуна внутрішнього згоряння або газового генератора. Можуть використовуватися і акумуляторні батареї, якщо їх потужності і часу роботи досить.

Для забезпечення першочергових потреб виділяються окремі «аварійні» енергетичні ланцюги. Життєво важлива чітка безперебійна робота енергетичної системи в медичних установах, транспортних вузлах і місцях скупчення людей, стратегічних об'єктах.

Локальне забезпечення електроенергією електронних компонентів беруть на себе джерела безперебійної енергії.

Система охорони для розумного дому, напрямлена на його автоматизацію, повинна виконувати багато різних функції. Як показано на рис.1, така вона помічає пожежу на ранніх стадіях завдяки сенсору температури, повідомляє про можливе затоплення або витік газу, а також обмежує можливість доступу до приміщень дому.

Рисунок 1.2 – Система охорони і автоматизації розумного дому

1.4 Системи відеоспостереження розумних будинків

Системи відеоспостереження як засіб охорони служать людському суспільству вже понад 70 років[3]. Вони працюють практично у кожному місті, магазині, банку. Навіть у менш розвинутих країнах ринок засобів відеоспостереження швидко зростає. Для збільшення якості спостереження, уже багато років ведуться розробки у сферах покращення якості відео і зйомки, кодування зображень, стрімінгу відео і збереження

та стиснення даних. Ці розробки збільшують ефективність відео нагляду, дозволяючи зберегти більше деталей використовуючи менше місця. Сучасні рішення стають все більш вигідними, компактними, водночас забезпечуючи більшу якість зйомки.

Підсистема відеоспостереження є однією з найважливіших компонент розумного дому. Зараз на ринку представлено багато рішень, є варіанти, що прив’язані до центральної системи дому, так і працюючі окремо від неї, і користувач може обрати систему собі до смаку: просту мережу IP камер, як з розумною обробкою відео так і без неї, систему прихованих камер, дротову або бездротову.

На ринку представлені такі варіанти систем спостереження:

В цій роботі пропонується модель однієї із підсистем системи охрони – системи спостереження навколишнього середовища. Під цим будемо розуміти взаємопов’язані відеокамери і сенсори, які слідкують за станом певної території і центральний комп’ютер, який зв’язує компоненти, обробляє дані і повідомляє власника про будь-які нештатні ситуації.

ADT's Home Security Starter Kit

Система охорони розумного дому, що працює на основі платформи Samsung's SmartThings. Постачається як набір компонентів, які користувач повинен самостійно розмістити в своєму домі. Складається з:

- ADT Security Hub, семи дюймового кольорового тачскріну, який слугує контролюючий пристроєм системи.
- Двох бездротових сенсорів стану вікна та дверей, сенсору руху та камери.
- Додаткової батареї, для підтримки безперебійного живлення при відсутності електропостачання.

Ціна початкового комплекту – $400. Камери відеоспостереження можна докуповувати окремо за ціною $70.

Vivint

Комплект складається з камери-вхідного дзвінка, двох відеокамер, розумних замків, термостату і системи контролю дверей гаража. Система здатна записувати відео 24/7, яке можна переглядати в мобільному додатку і зберігати дані усіх датчиків за довгий період часу.

Система потребує професійного встановлення, контроль усіх елементів (замків, дверей гаража, температури) здійснюється за допомогою мобільного додатку Vivint. Також через нього можна отримувати сповіщення про використання дверного дзвінка, відкриття дверей, переміщення всередині дому. Підтримуються голосові асистенти від Google та Amazon.

Ціна комплекту - $500, річна підписка обійдеться ще в $300, додаткові компоненти, як то камери, сенсори диму і газу, можна придбати окремо.

Xfinity

Система, що потребує професійного встановлення і пропонує 24/7 моніторинг, екстрену батарею, що гарантує роботу системи при перебоях в електропостачанні та панель керування, з якої можна віддавати команди окремими елементами дому.

Xfinity включає в себе сенсори відкриття дверей та вікон, сенсор руху та планшет, який слугує головним терміналом системи. Компанія пропонує доповнення системи: камери внутрішнього та зовнішнього спостереження, термостат, розумні крани та сенсори диму.

Система сумісна з багатьма приладами інших компаній, що пропонують рішення для розумного дому, наприклад з розумними замками August, контролерами дверей гаража Chamberlain, термостатами Nest та лампами Phillips.

Система постачається за умовою підписання 2 річного договору, який обійдеться в $720.

Проаналізувавши вищеописані системи, можемо виокремити їх основні недоліки:

- Закриті протоколи обміну даними, які роблять неможливим розширення і налаштовування системи компонентами інших виробників.
- Висока вартість продуктів і додаткових компонентів, система місячної підписки.
- Необхідність професійного встановлення системи, яка може бути недоступною в багатьох країнах.
- Обмежена можливість керувати відеоспостереженням, віддавати команди і реагувати на зміни середовища.

1.5 Системи відеоспостереження із використанням безпілотних літаючих апаратів

Дрони, також відомі як безпілотні літаючі апарати (БЛА) це машини, оснащені сенсорами, такими як камери, акселерометри, сенсори нахилу і магнітного поля, вимірювачами інерції. Дрони можуть контролюватися людиною оператором, так і працювати повністю або частково автоматично. Дрони це нова і швидко еволюціонуюча технологія, основним застосуванням якої донедавна була військова справа[4]. Та останнім часом сфера використання дронів росте надзвичайно швидко, БЛА проникають у все нові професійні та промислові середовища. Їх використовують рятувальні служби, для пошуку вижившихпід час рятувальних операцій, науковці, для проведення досліджень в сурових кліматичних умовах. Вони знайшли своє місце і в сфері безпеки, поліція та приватні охоронні компанії використовують дронів для спостереження за небезпечними ситуаціями без ризику для життя операторів.

Зараз на ринку не представлено жодної системи охорони середовища дому, яка б використовувала дрон в якості камери відеоспостереження, але є компанії, які обіцяють представити такі розробки вже найближчим часом.

Sunflower Home Awareness System

Компанія Sunflower розробляє новітню систему безпеки, що об'єднує розумні наземні сенсори з літаючою камерою. При появі нештатної ситуації користувач отримуватиме сповіщення на телефон і зможе відправити дрон-камеру, відео з якої транслюватиметься в додаток. Система оснащена здатністю до навчання, з часом вона знатиме звичайні маршрути жильців, зможе розпізнавати чужаків і відлякувати їх звуковими та світловими сигналами.

Рисунок 1.4.Реклама Sunflower Home Awareness System

Основним компонентом є сенсор Sunflower Smart Light, який суміщає в собі 360° сенсор руху, мікрофон, сенсор вібрацій і сонячну панель для зарядки батареї. Дрон оснащений GPS навігатором, автопілотом, камерою з високою роздільною здатністю і камерою для стабілізації зображення.

В комплекті постачається 4 сенсори, літаюча камера та мобільний додаток, з якого можна керувати системою. Оголошена ціна - $159 за один сенсор і $799 за камеру, випуск системи для тестування обіцяють в кінці 2018 року.

Були і невдалі спроби розробки систем із дронами-охоронцями: компанії Hawkeye та Aire пропонували покупцям профінансувати їх рішення за системою краудфандинг, але, не дивлячись на успішний збір коштів, проекти закрили, повернувши кошти клієнтам.

1.4 Постановка задачі

Отже, для забезпечення відео нагляду за навколишнім середовищем розумного дому, необхідно розробити ПЗ системи спостереження, яке інтегрується в існуючу систему автоматизації розумного будинку і об’єднує центральний контролер, сенсори та дрон в єдину систему моніторингу, що здатна реагувати на нештатні ситуації і повідомляти про них користувача. Для успішного проектування необхідно виконати такі задачі:

Поставити вимоги до розроблюваного ПЗ і на їх основі – вимоги до використовуваних технологій.

Провести аналіз можливих технологій розробки і потенціальних середовищ розгортання системи, вибрати такі, що задовольняють вимогам.

Розробити алгоритми роботи та архітектуру системи відеоспостереження розумного дому.

Розробити ПЗ.

РОЗДІЛ 2 ТЕХНОЛОГІЇ СТВОРЕННЯ СИСТЕМИ СПОСТЕРЕЖЕННЯ СТАНУ ТА ОБ'ЄКТІВ РОЗУМНОГО ДОМУ

2.1. Специфікація вимог до програмного забезпечення

Основою успішної розробки системи програмного є її специфікація. Чітко сформульована специфікація допомагає уникнути багатьох проблем в процесі розробки і цим зробити його більш простим.

На найвищому рівні абстракції система, що розробляється в даній роботі є набором програмних компонентів, що інтегруються в готове середовище керування розумним домом. Вони забезпечують зв'язок сенсорів, центрального серверу та мобільної платформи, пов'язуючи їх у систему спостереження.

Таке програмне забезпечення повинне реалізовувати наступні функції:

- підтримка постійного зв'язку із сенсорами, реєстрація показників та збереження їх у сховищі даних.
- обробка команд від користувача
- передача інструкцій дрону залежно від показників або команд користувача
- отримання відео потоку від дрона та його обробка
- надання можливості отримання відео потоку клієнтською частиною

2.2. Специфікація вимог до технологій розробки системи спостереження

Система спостереження повинна працювати в режимі реального часу для забезпечення постійного моніторингу середовища. Це ставить високу планку перед швидкодією технологій реалізації, адже затримки в обробці неприпустимі, вони можуть привести до порушення безпеки. потрібно аби система була здатна опрацьовувати потоки даних від багатьох незалежних джерел. Щоб забезпечити майбутню розширюваність системи, система має

одночасно опрацьовувати дані із багатьох сенсорів, що обумовлює пошук рішень, які дозволять реалізувати багато поточну обробку.

Будова і специфікація пристроїв, що входять до складу розумного дому, виходять за рамки цієї роботи, але, так як однією із цілей проекту є забезпечення відкритості системи і можливість підтримки пристроїв різних виробників, будуть дані загальні поради по вибору компонентів.

2.2.1. Одноплатний комп'ютер Raspberry Pi

Raspberry Pi — одноплатний комп'ютер створений з метою зробити вивчення інформатики доступним для всіх[3]. З часом він отримав набагато більш широке поле застосування і популярність, ніж очікували його творці. Основними причинами популярності є низька ціна, відкритість технологій, акцент на простоту освоєння та заохочення експериментів. Розробники регулярно випускають нові версії комп'ютера та програмного забезпечення, покращуючи характеристики компонентів.

На даний момент останньою версією є Raspberry Pi 3 Model B.

Таблиця 2.1

Характеристики Raspberry Pi 3 Model B

Ціна:	US$35
SoC:	BCM2835
CPU:	700 MHz ARM
GPU:	Broadcom VideoCore IV,OpenGL ES 2.0, 1080p30 H.264
Пам'ять (SDRAM):	512 MB
USB 2.0 порти:	2 (через інтегрований хаб)
Відео вихід:	Composite, HDMI
Аудіо вихід:	3.5 mm jack, HDMI
On-board storage:	SD/MMC/SDIO memory card slot
On-board network:	10/100 wired Ethernet
Low-level peripherals:	Up to 16 GPIO pins, SPI, I²C, UART

Властивості живлення:	700mA, (3.5 W)
Джерело живлення:	5V micro USB
Програмне забезпечення:	Debian GNU/Linux, Fedora
ПО, що підтримується:	Other FLOSS software (Iceweasel, KOffice, Python),RISC OS
Real-time clock:	None

Raspberry Pi став де-факто стандартом для побудови відкритих рішень автоматизації, через простоту освоєння та для нього розроблено багато приладів та додатків, які дозволяють налаштувати систему згідно бажань користувача.

2.2.2. Платформа openHAB

openHAB — відкритий проект домашньої автоматизації, націлений на створення універсальної платформи для об’єднання всієї розумної домашньої техніки в єдину платформу управління.

openHAB реалізує єдину шину, тобто дозволяє об'єднувати пристрої з різними протоколами в єдину мережу, абстрагуючи користувача від кожного конкретного протоколу. Таким чином, можна користуватися єдиним засобом управління (скажім, додатком на смартфоні) і реалізувати скільки завгодно складну логіку взаємозв'язку між пристроями.

openHAB надає розробнику зручне API для взаємодії із компонентами дому, що дозволяє писати комплексні додатки не вдаючись у деталі реалізації окремих частин системи.

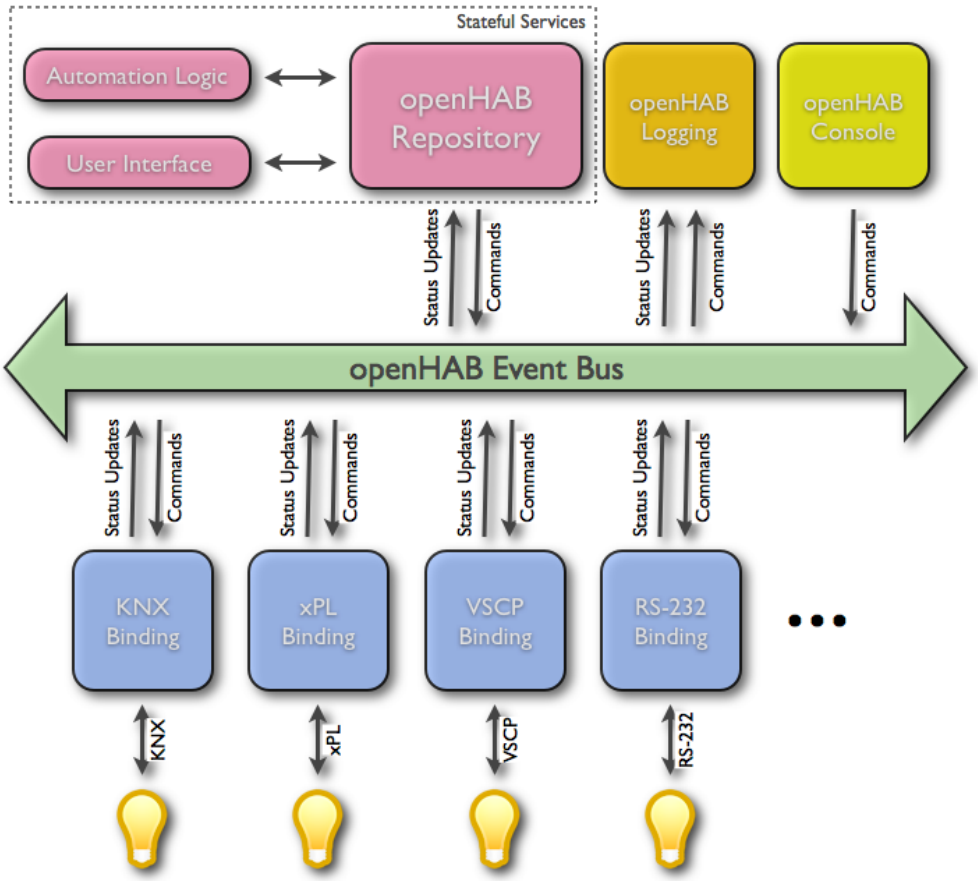

Рисунок 2.1. Архітектура openHAB

2.2.3. Мова програмування Go

Golang або Go —мова програмування, початок якій було покладено у 2007 році працівниками компанії Google: Кеном Томпсоном, Робом Пайком і Кеном Томпсоном. Go статично компільована і типобезпечна мова з багатою стандартною бібліотекою.

Мета створення Go була продиктована внутрішніми потребами компанії Google, вона розроблена для ефективної роботи на сучасних обчислювальних машинах, побудованих на багатоядерних процесорах і розподілених системах. Його можна розглядати як спробу створити заміну мов C та C ++ . По словах Роба Пайка[4], «Go була створена для вирішення реальних проблем, що виникають при розробці програмного забезпечення в Google». В якості основних таких проблем він називає:

- повільна компіляція програм

- неконтрольовані залежності
- складність розробки додаткових інструментів
- дублювання розробок

Go - компільована мова. Припускається, що програми на Go будуть транслюватися компілятором в об'єктний код цільової платформи і в подальшому виконуватися безпосередньо, не потребуючи віртуальної машини. Архітектура мови з самого початку була розроблена таким чином, щоб забезпечити швидку компіляцію в ефективний об'єктний код. Хоча для Go доступний і інтерпретатор, практично в ньому немає потреби, так як швидкість компіляції досить висока для забезпечення інтерактивної розробки.

Підтримка конкурентності в Go – одна із найважливіших її можливостей. Вона спроектована на основі Communicating Sequential Processes Тоні Хоара, формальної мови для опису моделей взаємодії в паралельних системах.

Модель багатопотоковості Go була розроблена на основі формальної мови для опису моделей взаємодії в паралельних системах CSP, запропонованої Тоні Хоаром. Це простий і одночасно потужний концепт, що робить написання конкурентних програм зручним і комфортним.

Новий потік виконання програми створюється використанням вбудованої функції go, яка запускає вибрану частину програми у новій горутині (так в Go називаються сопрограми). В межах одного процесу, горутини ділять спільний адресний простір, вони виконуються поверх потоків операційної системи не прив’язуючись до них. Рантайм середовище контролює розподіл горутин по віртуальних тредах, а тих в свою чергу – по реальних ядрах процесору. Це забезпечує гнучкість виконання, середовище може переміщувати горутини із заблокованих потоків на вільні. Вбудований мультиплексор дозволяє створювати дуже багато гору тин, кількість яких в рази більша доступних потоків. Горутини

спілкуються між собою використовуючи канали (один з типів стандартної бібліотеки), через які можна передавати будь-які типи даних.

З огляду на означені особливості Go можемо зробити висновок, що вона підходить для створення системи відеоспостереження розумного дому, мультиплатформенність забезпечує підтримку різних центральних контролерів, а швидкість виконання і підтримка багато потоковості забезпечать обробку даних від сенсорів і передачу команд іншим пристроям в режимі реального часу.

2.2.4 Фреймворк gRPC

gRPC (gRPC Remote Procedure Calls) це система виклику віддалених процедур (RPC) з відкрити кодом, розроблена компанією Google. Вона використовує HTTP/2 в якості транспорту, Protocol Buffers як інтерфейс мови опису взаємодії і надає такий функціонал, як аутентифікацію, двонапрямлений стрімінг і контроль потоку, блокуючі та не блокуючі виклики, таймаути. Є вбудовані інструменти для генерації крос-платформених клієнтських та серверних частин для багатьох мов програмування.

Основні переваги, які зумовлюють вибір gRPC як фреймворку зв’язу між компонентами, є:

- формат Protocol Buffer – мультимовний, багатоплатформений, розширюваний механізм для серіалізації структурованих даних. Він виконує функції XML: або JSON, але, при цьому, повідомлення займають менше місця, передаються швидше, опис структур даних спрощується. Це оптимальний вибір для високонавантаженої системи, що передає великі масиви даних.
- Асинхроні виклики дозволяють не блокувати мережу для отримання нового повідомлення, це дозволяє одночасно опрацьовувати декілька запитів і відповідати на них.

- Двонапрямлений стрімінг RPC – клієнт і сервер обмінюються метаданими, описами очікуваних структур повідомлень і відкривають дуплексне з'єднання. Вони можуть писати незалежно один від одного і обмінювати потоками повідомлень, змінюючи поведінку залежно від отриманих результатів, це робить gRPC ідеальним вибором для систем, які повинні підтримувати постійний зв'язок компоненті і реагувати на різні події в режимі реального часу.

2.3. Інструментальні засоби розробки ПЗ

Важко переоціни значення інструментів, якими користується розробник в процесі створення програмних систем. Вміло налаштоване середовище засобів забезпечує високу ефективність, збільшує швидкість розробки і спрощує процеси відлагодження продукту.

2.3.1. Середовище розробки Goland

Goland – нова комерційна IDE від компанії JetBrains, задача якої - надати той же рівень зручності при програмуванні на Go, який PyCharm забезпечує для Python, а IntelliJ IDEA - для Java. Ось деякі із її можливостей:

- Гнучка системи збору проекту на основі технології gobuild, компіляції в один натиск під всі підтримувані архітектури та операційні системи.
- Інтеграція технології профілювання Pprof, що дозволяє знаходити вузькі місця проекту і оптимізовувати їх.
- Шаблони коду для допомоги в створені типових додатків.
- Підтримка популярних систем контролю версій, таких як Git, SVN, Mercurial.
- Підтримка великої кількості доповнень від IntelliJ та сторонніх розробників.
- Вбудований помічник для Google Cloud Platform, який полегшує інтеграцію Cloud Video Intelligence та App Engine.

Враховуючи вище описані особливості, а також ергономічний дизайн, статичний аналіз коду і розумне доповнення, можемо зробити висновок, що GoLand – оптимальний вибір для створення систем мовою Go.

2.3.2. Bitbucket

Bitbucket (букв. «відро бітів») – веб-сервіс для хостингу проектів та їх спільної розробки, заснований на системі контролю версій Mercurial і Git. За призначенням і пропонованих функцій аналогічний GitHub (однак GitHub не надає безкоштовні «закриті» репозиторії, на відміну від Bitbucket), який підтримує Git і Subversion. Деякі особливості системи BitBucket:

В даний час всім користувачам безплатної версії пропонуються наступні можливості:

- Об'єм дискового простору до 2ГБ на репозиторій.
- Необмежена кількість публічних і приватних репозиторіїв.
- Доступ по протоколам HTTP(S) і SSH.
- Використання вбудованих система безперервної доставки, що дає можливість компілювати, тестувати та завантажувати на сервер в одному місці.
- Підтримка популярних сервісів організації роботи команд, таких як Trello, Slack, Jira.

Користуватися приватними (закритим) репозиторієм дозволено командам розміром до 5 користувачів. Більша кількість місць надається за умови оформлення платної підписки вартістю від $5 до $90 в місяць.

2.4. Архітектура системи

Одним із найістотніших етапів розробки будь-якої технічної системи є створення її архітектури, вона слугує фундаментом всього наступного процесу побудови. Якісна архітектура забезпечить легке масштабування і

гнучкість всього проекту, зменшить поріг входження для розробників та користувачів і навпаки, погано продумана архітектура зробить розробку складнішою: чим більшим ставатиме проект тим відчутнішими стануть перешкоди перед розробниками, добавлення нового функціонал буде більш незграбним і каверзним. Як результат, на якомусь з етапів розробки ми отримаємо програмний продукт, масштабування і доповнення якого стануть настільки затратними, що буде вигідніше почати процес створення з початку. Через це не буде перебільшенням твердження, що архітектура – це найважливіший модуль в процесі розробки, важливіший за функціонал, так як якісна архітектура гарантує підтримку впровадження нових можливостей в роботу системи.

Мікросервісна архітектура

«Мікросервіси» - ще один новий термін в мінливій сфері розробки ПЗ. Будь-яка нова технологія – це завжди невідома територія до якої варто ставитися досить насторожено, необхідно провести дослідження і оцінити ризики. Конкретно цей термін описує стиль розробки ПО, який світова спільнота знаходить все більш і більш привабливим. За останні кілька років було створено безліч проектів, що використовують цей стиль, і результати досі були досить позитивними. Настільки, що для багатьох компаній та команд по всьому світу цей стає основним стилем розробки ПО.

Немає єдиного формального визначення мікросервісної архітектури, існують певні характеристики, які допомагають нам зрозуміти цей стиль[7]. По суті, архітектура мікросервісу є методом розробки програмних додатків як набору незалежних для розгортання невеликих, модульних сервісів, в якій кожен сервіс запускається як унікальний процес і спілкується через чітко визначений, легкий механізм, що служить для досягнення бізнес-цілей.

Способи взаємодії сервісів між собою залежать від вимог вашої програми, але багато розробників використовують HTTP/REST за допомогою JSON або Protobuf. Професіонали DevOps, звичайно, можуть вільно вибирати будь-який комунікаційний протокол, який вони вважають підходящим, але в більшості випадків REST (Representational State Transfer) є корисним методом інтеграції через його простоту і універсальність.

Щоб краще осягнути ідею мікросервісів, варто згадати підхід, який був домінуючим в сфері розробки програмного забезпечення довгі роки – моноліт. Основна ідея монолітної архітектури в тому, що додаток будується як єдине ціле, всі частини якого запускаються одним процесом. Це прямолінійний і зрозумілий підхід до побудови, основними перевагами якого є простота розробки, розгортання і тестування, які можуть виконуватися розробником на власній машині, легкий процес масштабування додатку. Додаток-моноліт може благополучно виконувати свої функції, але з розповсюдженням хмарних технологій розміщення додатків, все більше користувачів відмовляється від цього підходу. Будь-яка модифікація системи потребує перебудовувати і викладати на сервер весь моноліт. В процесі розробки, задача збереження чистої модульної структури стає все важчою, модифікація логіки одного компоненту може призвести до зміни поведінки інших, для масштабування однієї із частин додатку необхідно дублювати всю систему.

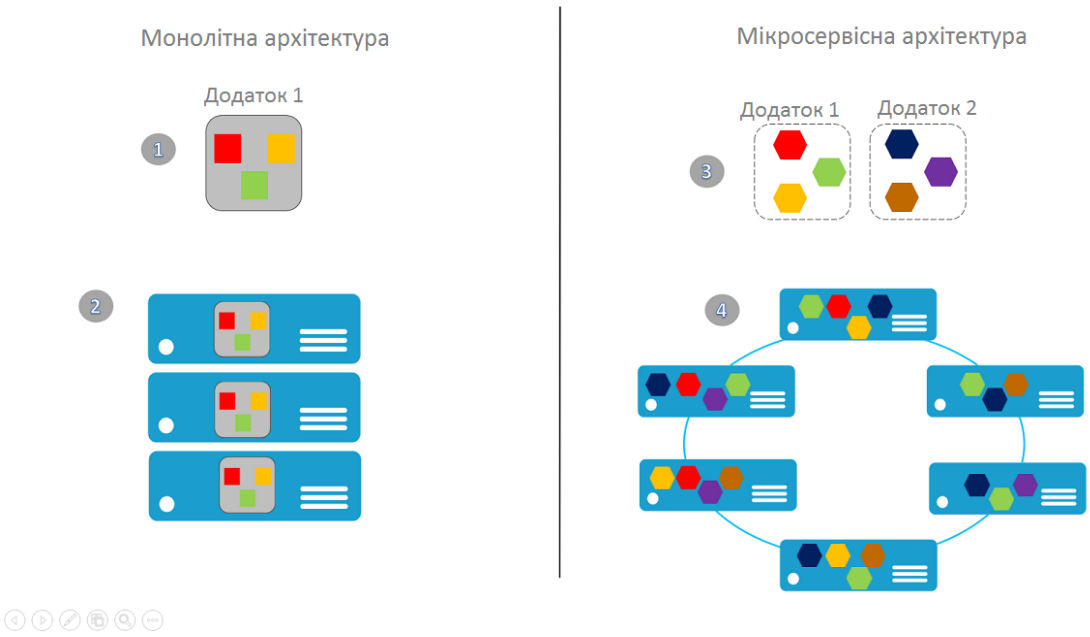

Рисунок 2.2. Порівняння монолітної та мікросервісної архітектур

Мікросервісна архітектура запропонована як ідея, націлена на вирішення недоліків моноліту. Спробуємо окреслити загальні характеристики мікросервісів:

- Розбиття на сервіси

Головна причина використання сервісів, а не пакетів, це можливість викладати на сервери окремо кожен із компонентів. Це робить частини незалежними одна від одної, модифікація однієї із них не призводить до змін логіки інших (хоча й може знадобитися переробити договорености між сервісами).

- Організація навколо вимог бізнесу

При розробці моноліту, звичайною практикою є розподіл команд розробки по використовуваних технологіях, наприклад команда розробки інтерфейсів користувача, команда бекенду, команда баз даних. Це призводить до проблем з інтеграцією їх розробок навіть при невеликих змінах, через необхідність взаємодії між різними командами. Мікросервісний стиль заохочує створення команд, які працюють над вирішенням єдиної бізнес задачі, що спричинює формування команд з професіоналів в різних областях.

- Децентралізоване керування даними

Модель предметної області може відрізнятися у різних команд розробки одного продукту, одне поняття може розглядатися з декількох позицій, що призводить до різниці в його представленнях. Монолітні додатки зазвичай використовують єдину базу даних, збереження в ній різних моделей об’єктів може привести до надлишковості Мікросервісна архітектура дає змогу кожному сервісу керувати своєю базою даних, яка зберігає саме те представлення, яке необхідне для реалізації бізнес потреби.

Не дивлячись на усі переваги мікросервісів, вони не стали універсальним рішенням усіх проблем, що постають перед архітекторами систем. Цей підхід змушує розробників вирішувати ряд нових проблем.

- Комплексність. Мікросервісне рішення складається з більшої кількості компонентів, ніж монолітний аналог. Кожен окремий сервіс простіший, ніж у моноліті, але система в цілому стає складнішою.
- Цілісність даних. Так як кожен сервіс відповідає за збереження даних, забезпечення цілісності може бути проблемою.
- Затримки мережі. Використання багатьох невеликих сервісів призводить до інтенсивнішого числа взаємодій між ними. Зі зростанням кількості взаємодій у системі мережеві затримки можуть стати проблемою.

Проаналізувавши особливості мікросервісної і монолітної архітектур, можемо прийти висновку,

РОЗДІ 4. ОХОРОНА ПРАЦІ

Охорона праці – це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-

профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності [1].
Дипломний проект на тему «Комплекс задач формування комплекту спорядження персонажу браузерної MMORPG-гри» пов’язаний з комп’ютерним моделюванням та розробкою програмного забезпечення.

В даному розділі описано робоче місце адміністратора, що обслуговуватиме веб-застосування з урахуванням необхідних показників і встановлених норм. Працюючи за комп'ютером, людина потрапляє під вплив різноманітних факторів: електромагнітних полів (діапазон радіочастот: ВЧ, УВЧ і СВЧ), інфрачервоного та іонізуючого випромінювання, шуму і вібрацій, статичної електрики. Розділ включає аналіз мікроклімату, освітлення, опис інструкції пожежної безпеки приміщення, в якому буде відбуватися робота адміністратора.

6.1 Характеристика робочого місця

Робоче місце адміністратора знаходиться в одній із комп’ютерних лабораторій, яка обладнана для роботи одного працівника. Лінійні розміри становлять 3,5 м × 2,5 м, висота стелі 2,6 м. (таблиця 6.1). Площа та об’єм приміщення зазначені в таблиці 6.2.

Таблиця 6.1 – Розміри приміщення

Довжина, м (L)	3,5
Ширина, м (D)	2,5
Висота, м (H)	2,6

Таблиця 6.2 – Площа та об’єм приміщення

Геометрична характеристика	Одиниця виміру	Нормативне значення	Фактичне значення
Площа, S	$м^2$	не менш 6.0	8,75
Об’єм, V	$м^3$	не менш 20	22,75

За даними, що наведені вище у таблиці 6.2, можна зробити висновок, що геометричні розміри приміщення відповідають правилам [2].

Основним робочим положенням є положення сидячи. Головними елементами робочого місця є письмовий стіл, крісло і комп’ютер.

З меблів в лабораторії знаходиться один кутовий стіл, одне крісло, дві шафи з документами та прямокутний стіл для розташування іншої техніки. З техніки наявні один персональний комп’ютер, принтер та телефон.

План приміщення зображено на рисунку 6.1. На ньому цифрами позначено наявні елементи: 1 – кутовий стіл; 2 – прямокутний стіл; 3 – крісло; 4,5 – шафи; 6 – монітор; 7 – телефон; 8 – принтер.

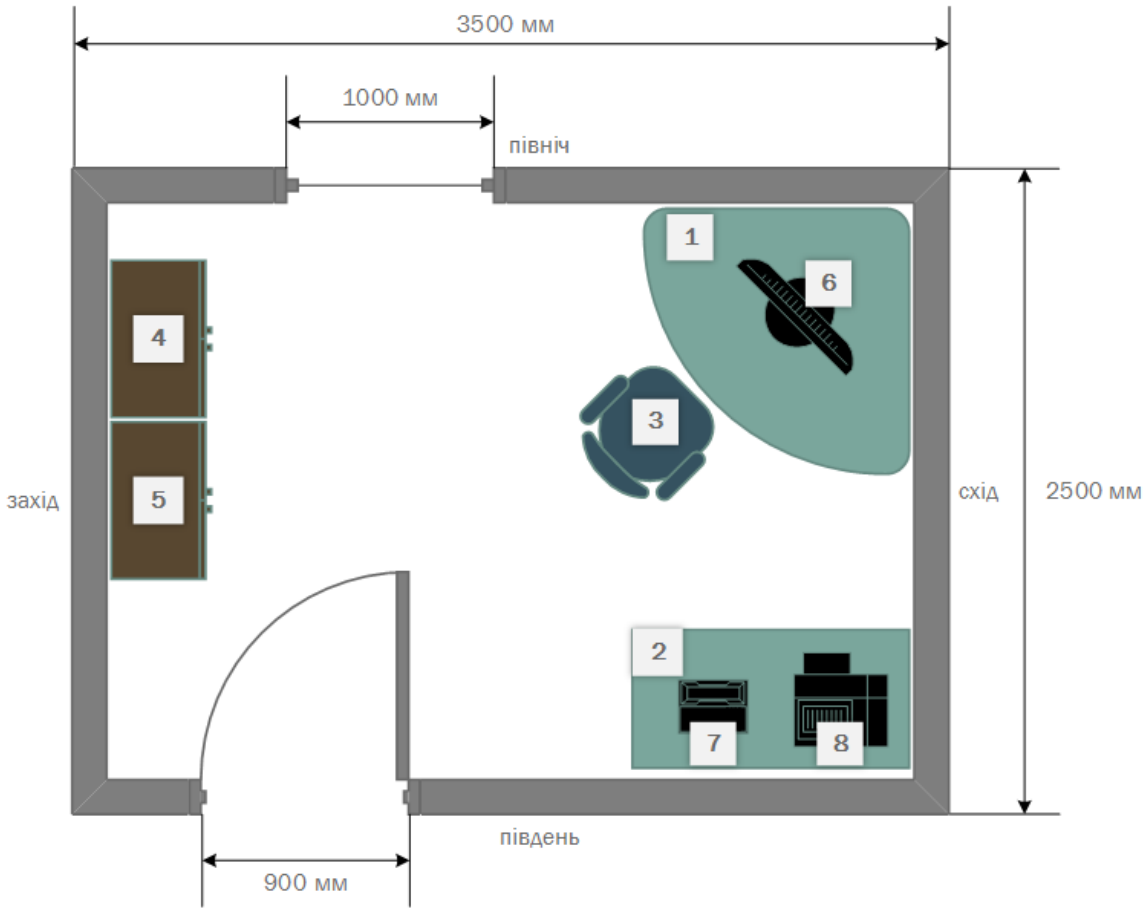

Рисунок 6.1 – Спрощений план приміщення

6.2 Аналіз і оцінка шкідливих виробничих факторів

Розглянемо робоче місце користувача ПК з точки зору оцінки впливу шкідливих виробничих факторів відповідно до гігієнічної класифікації праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу [3]. Відповідно до цього документу, на працівника, який працює з комп'ютером діють такі шкідливі виробничі чинники: мікроклімат робочої зони; шум; випромінювання; недостатність штучного освітлення та пожежонебезпека.

6.2.1 Мікроклімат робочої зони

В приміщенні використовується центральна система водяного опалення низького тиску.

Оскільки робота виконується сидячи та без фізичного навантаження, то її категорія оцінюється як «легка-1а». Відповідно до встановлених вимог [4] роботодавець зобов'язаний забезпечити в приміщеннях для даного типу роботи оптимальні параметри виробничого середовища (таблиця 5.3).

Причиною підвищеної температури робочої зони можуть бути освітлювальні пристрої, величина тепловиділення яких становить 35-60 Вт/м^2, а також комп'ютер, середня величина тепловиділення якого становить 310 Вт/м^2.

Таблиця 6.3 – Норми мікроклімату для приміщень з ЕОМ

Пора року	**Параметр мікроклімату**	**Оптимальне значення**	**Фактичне значення**
Холодна	Температура повітря	22-24°С	23°С
	Відносна вологість повітря	60 - 40%	31%
	Швидкість руху повітря	0,1м/с	0,1м/с
Тепла	Температура повітря	23 - 25°С	24,5°С
	Відносна вологість повітря	60 - 40%	58%
	Швидкість руху повітря	0,1 м/с	0,1м/с

6.2.2 Шум

На комп'ютеризованих робочих місцях основними джерелами шуму є вентилятори системного блоку та принтери. Сильний шум викликає

труднощі з розпізнаванням колірних сигналів, знижує швидкість сприйняття кольорів, гостроту зору, зорову адаптацію, порушує сприйняття візуальної інформації, зменшує на 5-12% продуктивність праці.

На даному робочому місці основними джерелами шуму є вентилятори системи охолодження системного блоку комп'ютера, а також принтери та телефон. Також варто врахувати шум, що надходить ззовні, і який ліквідується використанням акустичних поглиначів звуку, а також вікон, що щільно закриваються.

Для покращення робочої обстановки необхідне технічне вдосконалення та періодичне обслуговування системних систем охолодження комп'ютерів. А принтери перемістити за межі лабораторії, або помістити в звукоізоляційну коробку.

Розрахуємо рівень шуму в приміщені. Величина рівня шуму типових джерел надано в таблиці 6.4.

Таблиця 6.4. Значення рівня шуму для типових джерел

Джерело шуму	**Рівень шуму, дБА**
Жорсткий диск	30
Вентилятор	45
Монітор	15
Клавіатура	8
Принтер	40
Телефон	45

Максимальний час роботи принтера за один день – 1,5 години.

Робочий день T = 8 годин. Розрахуємо фактичний рівень шуму за наступною формулою.

$$L_{\Sigma} = 10\lg(10^3 + 10^{4,5} + 10^{1,7} + 10^{0,8} + 10^4 + 10^4) = 48{,}7 \text{ дБА}$$

Під час роботи за комп'ютером рівень шуму відповідно до норм [5] не повинен перевищувати 50 дБА, а фактичний становить 48,7 дБА. Отже, наше приміщення відповідає діючим санітарним нормам.

6.2.3 Випромінювання

Дисплей ПК є джерелом сильного електромагнітного випромінювання. Крім електромагнітних полів та випромінювання безпосередньо від монітора, на користувача додатково впливають так звані фонові поля – поля від сторонніх джерел, які знаходяться у приміщенні або поблизу від нього. Такими джерелами є мережі живлення і освітлення, побутові прилади (кондиціонер, обігрівач), мобільні телефони, бездротова мережа тощо.

Відповідно до [2], припустима інтенсивність потоку енергії 10 Вт/м^2, а напруженість електричного поля в електричній складовій на відстані 0,5 м. від екрану – 10 В/м. В сучасних LCD дисплеїв інтенсивність потоку складає не більше 1 Вт/м^2, а значить умови відповідають встановленим нормам.

6.2.4 Освітлення

Для запобігання прямого відблиску світла дисплеї розміщуються боком до вікна. Під час роботи в приміщенні, близько 75% всього часу погляд працівника спрямований в напрямку робочої поверхні, тобто в напрямку

дисплея. Розряд робіт – високої точності (через відносно невеликі розміри знаків на дисплеї), а фон – світлий.

В приміщенні використовується бокова система природного освітлення та загальна система штучного освітлення. Через це нормоване значення освітлення повинно бути 300 лк, а КПО становить 1.5. Коефіцієнт пульсації не перевищує 5%, що задовольняє вимогам [6].

Фактична площа вікон 1,5 $м^2$, що не відповідає чинним вимогам, тому в приміщенні застосовується освітлення з допомогою ламп денного світла.

Для освітлення приміщення використаний світильник з дзеркальними параболічними решітками, укомплектований електронним пускорегулюючим апаратом (ЕПРА). Світильник з ЕПРА має дві випереджальні та дві відстаючі гілки. Світильник розташовано над робочим місцем адміністратора (рисунок 6.2), а його характеристики такого світильника наведено в таблиці 6.5.

Таблиця 6.5 – Характеристики світильника

Назва	**Потужність, Вт**	**Струм, А**	**Напруга, В**	**Габаритні розміри, мм**	**Світловий потік, лм**	**Термін служби, годин**
Світильник LM160	160	0,73	220	38×1514,2×1500	6000	10000

6.3 Електробезпека

Трансформатор від якого живиться приміщення розташований поза ним, напруга на його первинній обмотці: 6.3 кВ, на вторинній: 380 В.

Режим нейтралі відносно землі – заземлений, режим електричної мережі – однофазний.

Електрична проводка виконана: мідним проводом в поліхлорвініловій ізоляції, площа поперечного розрізу 4 мм^2.

Живлення електрообладнання здійснюється напругою 220В.

Підвищена електрична небезпека наявна в приміщенні, якщо воно відповідає таким критеріям:

- відносна вологість повітря більше 75%;
- наявність струмопровідного пилу;
- наявність агресивного хімічного чи біологічного середовища, яке може стати причиною руйнації ізоляції;
- температура повітря більше 35°С;
- наявна можливість торкання до заземлених металевих конструкцій і струмопровідних частин водночас;
- наявність струмопровідної підлоги.

Оскільки, дане приміщення не відповідає наведеним вище критеріям, то воно не відноситься до групи із підвищеною електричною небезпекою.

Електробезпека приміщення забезпечується технічними способами і засобами захисту, а також організаційними заходами.

Всі елементи електроприладів й устаткування виконані відповідно до умов техніки електробезпеки, мають необхідне ізоляційне покриття (подвійна ізоляція) і властивості, що виключає можливість ураження електричним струмом при підключенні й експлуатації устаткування. Розетки змонтовані на негорючих пластинах і мають сучасну триконтактну конструкцію, захист виконаний у вигляді бічних контактів, які взаємодіють першими, при включені вилки в розетку й відключаються останніми при витягуванні вилки з розетки, що відповідає умовам [3].

Зважаючи на все вищевказане, за класом небезпечності приміщення відноситься до приміщень без підвищеної небезпечності.

6.4 Пожежна безпека

В приміщенні знаходяться пожежонебезпечні матеріали: папір (документація) та дерево (столи). Вибухонебезпечні матеріали у приміщенні відсутні.

Виходячи з властивостей та кількості пожежо- та вибухонебезпечних матеріалів за нормативною документацією [7] приміщення має категорію В.

Можливі причини виникнення пожежі – короткі замикання у комп'ютерах, підвищення температури в приміщенні або поява розжарених матеріалів.

Біля дверей розміщено план евакуації з даного приміщення на вулицю.

6.4.1 Засоби пожежогасіння

Приміщення обладнане двома вогнегасниками: ВВ-3,5 (кожен містить 3,5 кг вогнегасної речовини).

Відстань між місцями розташування вогнегасників не повинна перевищувати 15 м. В приміщенні знаходяться два вогнегасники (для зручності позначені індексами на схемі). Вогнегасники знаходяться на відстані один від одного, що відповідає нормам (відстань між першим і другим вогнегасником становить 3,22 метра).

6.4.2 Пожежна сигналізація

Згідно з додатком К до норм [8], в приміщенні встановленні димові датчики автоматичного знаходження пожежі ІПК-2. Датчики під'єднанні до центрального пульту охорони та безпеки.

6.5 Інструкція з техніки безпеки

Під час роботи, пересвідчившись у справності обладнання, увімкнути електроживлення ПК, розпочати роботу, дотримуючись умов інструкції з його експлуатації.

Забороняється:

- замінювати змінні елементи або вузли та проводити перемонтаж при ввімкненому ПК;
- з'єднувати і роз'єднувати вилки та розетки первинних мереж електроживлення, які знаходяться під напругою;
- знімати кришки, які закривають доступ до струмопровідних частин мережі первинного електроживлення при ввімкненому обладнанні;
- користуватися паяльником з незаземленим корпусом;
- замінювати запобіжники під напругою;
- залишати ПК у ввімкненому стані без нагляду.

Після закінчення роботи на ПЕОМ працівник повинен дотримуватись такої послідовності вимикання обладнання:

- здійснити закриття всіх активних завдань;
- вимкнути живлення системного блоку;
- вимкнути живлення всіх периферійних пристроїв;
- штепсельні вилки витягнути з розеток;
- накрити клавіатуру кришкою.
- про всі недоліки, що виявились у процесі роботи повідомити керівника робіт.

Висновки до розділу

У результаті проведеного аналізу умов безпеки праці на робочому місці працівника були виявлені шкідливі і небезпечні фактори, а також визначені та запропоновані варіанти вирішення його недоліків.

Було проведено розрахунок рівня шуму в приміщені та було встановлено, що він задовольняє нормам.

Окрім цього були розглянуті інструкції з охорони праці, питання пожежної безпеки та визначено необхідні умови для її забезпечення.

В результаті недотримання умов безпечної праці на робочу місці, у працівників спостерігається незадоволеність роботою, головний біль, роздратування, порушення сну, втома і больові відчуття в очах, попереку, у ділянці шиї та рук.

ПЕРЕЛІК ПОСИЛАНЬ

1. Kyas, Othmar. 2013. How To Smart Home. Key Concept Press.
2. https://www.protectamerica.com/home-security-blog/just-for-fun/home-alarm-industry-statistics-just-how-big-is-the-industry_16263
3. W. Dornberger, “V-2, ballantine books,” in ASIN: B000P6L1ES, 1954, pp. 14 – 15.
4. Ehsani & Maja, 2013; Gago et al., 2015).
5. https://uk.wikipedia.org/wiki/Raspberry_Pi
6. Go at Google: Language Design in the Service of Software Engineering https://talks.golang.org/2012/splash.article
7. https://www.martinfowler.com/articles/microservices.html