МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ

До захисту допускається
Завідувач кафедри
_____ Скарга-Бандурова І.С.
«____»_____ 20__ р.

МАГІСТЕРСЬКА РОБОТА

НА ТЕМУ:

Комп'ютерна система моніторінгу та управління навчальним закладом

Освітньо-кваліфікаційний рівень "Магістр"
Спеціальність 123 "Комп'ютерна інженерія" (освітня програма - "Комп'ютерні системи і мережі")"

Науковий керівник роботи:	_____ (підпис)	В.М.Барбарук (ініціали, прізвище)
Консультант з охорони праці:	_____ (підпис)	Я.О.Критська (ініціали, прізвище)
Студент:	_____ (підпис)	І.О.Дерябін (ініціали, прізвище)
Група:		КСМ-16зм

Сєвєродонецьк 2018

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет Інформаційних технологій та електроніки
Кафедра Комп'ютерних наук та інженерії
Освітньо-кваліфікаційний рівень магістр
Напрям підготовки _____
(шифр і назва)
Спеціальність 123 "Комп'ютерна інженерія" (освітня програма - "Комп'ютерні системи і мережі")
(шифр і назва)

ЗАТВЕРДЖУЮ:

Завідувач кафедри _____
_____ І.С. Скарга-Бандурова
«_____» _____20____р.

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

Дерябіну Ігорю Олександровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Комп'ютерна система моніторінгу та управління навчальним закладом

керівник проекту (роботи) Барбарук Віктор Миколайович, к.т.н., доц.
(прізвище, м.'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від «18» 10 2018 р. № 208/48
2. Строк подання студентом роботи 21.01.2018
3. Вихідні дані до роботи Матеріали науково-дослідної практики, структура та функції вищого навчального закладу, засоби інтернет речей

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Огляд технології інтернет речей, управління діяльністю вищого навчального закладу, автоматизація освітлення і системи контролю доступу, програмна та апаратна реалізація системи управління, охорона праці та безпека в надзвичайних ситуаціях,висновки

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

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці та безпека в надзвичайних ситуаціях	Критська Я.О. ст.викл. кафедри КНІ		

7. Дата видачі завдання 18.10.2017

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз літературних джерел і обґрунтування актуальності	10.09.2017-15.09.2017	
2	Розробка технічного завдання	16.09.2017-22.09.2017	
3	Огляд типової структури ВНЗ	23.09.2017-25.09.2017	
4	Програмна та апаратна реалізація ситсеми автоматизованого освітлення та системи контролю доступу	26.09.2017-06.10.2017	
5	Огляд методів та засобів інтернет-речей	07.10.2017-13.11.2017	
6	Розробка частини проекту "Охорона праці та безпеки в надзвичайних ситуаціях"	14.11.2017-30.11.2017	
7	Оформлення пояснювальної записки та презентації	01.12.2017-31.12.2017	
8	Оформлення автореферату	01.01.2018 – 10.01.2018	

Студент _____ Дерябін І.О.
(підпис) (прізвище та ініціали)

Науковий керівник _____ Барбарук В.М.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дерябін І.О. Комп'ютерна система моніторінгу та управління навчальним закладом.

Метою магістерської роботи є підвищення ефективності організаційно-технічного управління комплексною безпекою, системою контролю доступу, а також енергопостачанням ВНЗ шляхом розробки відповідного методичного та алгоритмічного забезпечення використовуючи технології інтернет речей. На підставі проаналізованих джерел та вивчення технології були запропоновані декілька варіантів оптимізації для управління вищім навчальним закладом.

Ключові слова: інтернет речей, датчик, мережа, моніторинг доступ.

THE ABSTRACT

Derjabin I.O. Computer system of monitoring and management of an educational institution.

The purpose of the master's thesis is to increase the efficiency of organizational and technical management of integrated security, access control and energy efficiency of the university by developing appropriate methodological and algorithmic support using IoT. Based on the analyzed sources and technology of Internet of things several optimizing variants for management of higher education institutions were proposed.

Key words: internet of things, sensor, network, monitoring, access.

АННОТАЦИЯ

Дерябин И.А. Компьютерная система мониторина и управления учебным заведением

Целью магистерской работы является повышение эффективности организационно-технического управления комплексной безопасностью, системой контроля доступа и энергоэффективностью ВУЗа путем разработки соответствующего методического и алгоритмического обеспечения с использованием технологии интернета вещей. На основании проанализированных источников и изучении технологии были предложены несколько вариантов оптимизации для управления высшим учебным заведением.

Ключевые слова: интернет вещей, датчик, сеть мониторинг, доступ.

ЗМІСТ

ВСТУП

Вже нікого не здивуєш тим, що будь-який предмет, будь то побутова техніка чи одяг, можуть бути підключені до інтернету. Розумний холодильник, чайник, конструктори для навчання дітей і інші. Поки одні підключають до всесвітньої павутини кавоварку, годинники та інші речі, інші дивуються, навіщо ускладнювати прості у використанні предмети і техніку. Чим же насправді є інтернет речей і чи може він бути нам корисний?

Інтернет речей (англ. Internet of Things, IoT) концепція обчислювальної мережі фізичних об'єктів (речей), оснащених вбудованими технологіями для взаємодії один з одним або з зовнішнім середовищем, яка розглядає організацію таких мереж як явище, здатне перебудувати економічні та суспільні процеси, що виключає з частини дій і операцій необхідність участі людини. Ідея Інтернету речей складається зовсім не в тому, щоб підключити до Інтернету всі навколо. Завдання автоматизувати процеси і навчити підключені до мережі предмети обмінюватися інформацією. Як? Через різні датчики, вбудовані або підключення до об'єктів. Навіщо? Щоб об'єкти самі приймали рішення і діяли без участі людини.

Майже класичний, вже сьогодні працює приклад реалізації інтернету речей Google Maps. Безліч автомобілів, оснащених Google Maps, відправляють свої координати, швидкість і напрямок в систему. Інформація обробляється і на карті видно не тільки дороги, але і їх завантаженість в реальному часі. Завдяки цьому навігатори можуть прокладати маршрут, враховуючи не тільки відстані, але і пробки. Це новий етап розвитку Інтернету, який значно розширює можливості збору, аналізу та розподілу даних, які людина може перетворити в інформацію, знання і, в кінцевому підсумку, в мудрість. У цьому сенсі Інтернет речей набуває величезне значення. Уже є проекти, які наочно показують його здатність подолати розрив між багатими і бідними, надати світові ресурси тим, хто найбільше їх потребує, і допомогти нам краще зрозуміти свою планету, щоб навчитися попереджувати проблеми. Разом з тим є фактори, що уповільнюють розвиток Інтернету речей. До них відносяться перехід до протоколу IPv6, прийняття єдиного набору загальних стандартів і розробка джерел живлення для мільйонів (і навіть мільярдів) мініатюрних датчиків.

Ідея об'єднання комп'ютерів, датчиків і мереж для відстеження і контролю пристроїв обговорювалася протягом десятиліть, проте недавнє злиття ключових технологій і тенденції на ринку відкрили нову реальність Інтернету речей. IoT обіцяє ввести нас в революційний, повністю інтегрований «розумний» світ, де зв'язок між

предметами і їх оточенням, а також між предметами і людьми стає все тісніше. Перспектива Інтернету речей як всюдисущої мережі пристроїв, прив'язаних до Інтернету, може фундаментально змінити уявлення людей про те, що значить перебувати в мережі.

Потенційні складності значні і безліч потенційних проблем може перегородити шлях цьому баченню, особливо в сферах безпеки, конфіденційності, інтероперабельності та стандартів, в тому числі в країнах, що розвиваються. Інтернет речей піднімає складний і зростаючий комплекс технологічних, соціальних і політичних проблем серед самих різних кіл зацікавлених осіб. Інтернет речей існує тут і зараз, і сьогодні спостерігається потреба знаходити власні шляхи розв'язання, пов'язаних з ним проблем і максимального використання його переваг з одночасним зменшенням ризику.

Таким чином, ця дослідницька робота присвячена актуальній науково-технічної задачі застосування технології Інтернету речей для вирішення широкого спектра завдань, починаючи від контролю за власним будинком і закінчуючи управлінням підприємством, а саме вищим навчальним закладом.

Метою магістерської роботи є підвищення ефективності організаційно-технічного управління комплексною безпекою, системою контролю доступу, а також енергопостачанням ВНЗ шляхом розробки відповідного методичного та алгоритмічного забезпечення. **Об'єктом дослідження** є вищий навчальний заклад, а **предметом** - оптимізація споживання ресурсів ВНЗ з використанням технології Інтернету речей.

Для досягнення поставленої мети **необхідно вирішити** такі завдання:

– проаналізувати концепцію Інтернету речей та її можливості;

– проаналізувати структуру ВНЗ і виконати огляд літератури для пошуку ефективних варіантів оптимізації роботи ВНЗ;

– розробити варіанти автоматизації господарської діяльності ВНЗ;

– реалізувати web-додаток для дистанційного керування освітлювальними приладами.

Публікації. Основні результати магістерської роботи доповідались на Всеукраїнській науково-практичній конференції «Електронні апарати та системи. Проблеми створення. Перспективи розвитку».

Практичне значення: запропоновані декілька варіантів оптимізації системи автоматизовано освітлення та системи контролю доступу.

Структура та обсяг роботи. Магістерська робота складається зі вступу, 5 розділів, висновків, переліку джерел, додатків. Загальний обсяг складається з 100 сторінок, 6 таблиць, 24 рисунків.

1 ОГЛЯД ТЕХНОЛОГІЇ ІНТЕРНЕТ РЕЧЕЙ

Інтернет речей (IoT) - важлива тема в сфері ITтехнологій, яка активно обговорюється як в спеціалізованій літературі, так і в широкій пресі. Ця технологія втілена в широкому наборі мережевих продуктів, систем і датчиків, які застосовують досягнення в області обчислювальної техніки, мініатюризації електроніки та мережевих з'єднань для інтеграції нових функцій, які раніше не були можливі. На численних конференціях, в звітах і пресі обговорюється можливий вплив «революції IoT», від нових ринкових можливостей і моделей бізнесу до проблем безпеки, конфіденційності та технічної інтероперабельності.

Великомасштабне використання механізмів IoT багато в чому змінить наш стиль життя. Для споживачів нові продукти IoT, такі як побутова техніка з підключенням до Інтернету, компоненти домашньої автоматики і пристрої для регулювання електроенергії наближають нас до концепції «розумного будинку», забезпечуючи більш високий рівень безпеки та енергоефективності. Інші особисті пристрої IoT, такі як носяться пристрої для фітнесу і контролю за станом здоров'я, а також медичні пристрої з підключенням до мережі змінюють методи надання медичних послуг. Перевагами цієї технології зможуть скористатися інваліди та люди похилого віку, так як вона здатна забезпечити більш високий рівень незалежності та якості життя за розумною ціною. Такі системи IoT як, транспортні засоби, підключені до єдиної мережі, інтелектуальні системи управління дорожнім рухом та вбудовані датчики на дорогах і мостах наближають нас до ідеї «інтелектуальних міст» для зниження числа пробок і скорочення енергоспоживання. Технологія IoT забезпечує можливість трансформувати сільське господарство, промисловість, виробництво і споживання електроенергії шляхом збільшення доступності інформації по всьому ланцюжку доданої вартості на виробництві з використанням мережевих датчиків. Однак для того, щоб скористатися всіма перевагами IoT, необхідно взяти до уваги і вирішити ряд питань.

Ряд компаній і науково-дослідних організацій роблять численні прогнози щодо потенційного впливу IoT на Інтернет і економіку протягом найближчих п'яти або десяти років. Наприклад, згідно з прогнозами Cisco, до 2019 року буде налічуватися 24 млрд об'єктів, підключених до Інтернету. Зі свого боку, Morgan Stanley прогнозує до 2020 року 75 млрд таких устройств. Huawei заглядає ще далі і прогнозує 100 млрд пристроїв з підключенням IoT до 2025 року. McKinsey Global Institute вважає, що фінансовий вплив IoT на глобальну економіку може досягти від 3,9 до 11,1 млрд. доларів к 2025 р.

Незважаючи на велику кількість прогнозів і неможливість визначити точні показники, в цілому вони вселяють перспективу значного зростання і впливу.

Деякі оглядачі вважають IoT символом світу повністю взаємоз'єднання пристроїв, прогресу, ефективності і широких можливостей, а також потенційним підвищенням цінності для промисловості і глобальної економіки, що виражається в мільярдах. Інші попереджають, що IoT є передвісником похмурого світу постійного спостереження, порушень конфіденційності та безпеки, а також залежно споживачів. Увага громадськості привернули заголовки в пресі про злом автомобілів, підключених до мережі Інтернет, заклопотаність постійним наглядом, заснована на функціях розпізнавання голосу в «інтелектуальних» телевізорах і побоювання щодо конфіденційності в зв'язку з потенційним зловживанням даними IoT. Це обговорення можливостей в порівнянні з ризиками, в поєднанні з постійною появою інформації в популярних ЗМІ і маркетингом можуть ускладнити розуміння IoT.

В цілому можна сказати, що Інтернет-спільнота цікавиться IoT, так як ця технологія являє розвивається аспект взаємодії людей і організацій з Інтернетом в особистому, суспільному та економічному житті. Навіть якщо найскромніші прогнози виявляться вірними, численні області застосування IoT можуть привести до фундаментальних змін у взаємодії користувачів з Інтернетом і його впливу на них. У свою чергу, це призведе до виникнення нових проблем і до нового погляду на вже існуючі проблеми, що турбують користувачів і споживачів, в області технології, політики і законодавства. Ймовірно, IoT також буде надавати різний вплив на різні економіки і регіони, відкривати різні можливості і ставити різні проблеми в усьому світі.

Дана робота сприяє членам спільноти Інтернету речей в підтримці діалогу з цього питання з урахуванням різних прогнозів щодо його потенційних небезпек і переваг. Вона включає компетентний короткий огляд основних характеристик IoT і деяких ключових питань, а також проблем, які ставить ця технологія по відношенню до Інтернет-спільноти і нашим основним цінностям. У даній аттестаційній роботі також розглядаються деякі унікальні аспекти Інтернету речей, завдяки яким ця технологія здатна трансформувати Інтернет.

1.1 Походження, визначальні чинники та області використання Інтернета речей

Термін Інтернет речей (IoT) вперше використав в 1999 році британський новатор в області технологій на ім'я Кевін Ештон для опису системи, в якій предмети фізичного світу можуть підключатися до Інтернету за допомогою датчіков.Ештон створив цей термін для того, щоб проілюструвати потенційні можливості підключення міток радіочастотної ідентифікації (RFID), які використовуються в корпоративних ланцюжках поставок, для підрахунку та відстеження товарів без необхідності втручання з боку людини. Сьогодні термін Інтернет речей широко використовується для опису сценаріїв, в яких підключення до Інтернету і обчислювальні функції поширюються на ряд об'єктів, пристроїв, датчиків і інших предметів повсякденного життя.

Незважаючи на те, що термін Інтернет речей є порівняно новим, концепція об'єднання комп'ютерів і мереж для моніторингу та управління пристроями існує вже кілька десятиліть. Наприклад, уже в кінці 1970-х рр. здійснювалося комерційне використання систем для віддаленого моніторингу лічильників електричної мережі через телефонні лінії. У 1990-х рр. досягнення в області бездротової технології зробили можливим широке поширення корпоративних і виробничих рішень «машина-машина» (M2M) для моніторингу та управління обладнанням. Однак багато хто з цих ранніх рішень M2M були створені на основі закритих спеціалізованих мереж на фірмових або галузевих стандартах, а не на мережах на основі протоколу Інтернету (IP) і стандартах Інтернету.

Ідея використання IP для підключення до Інтернету пристроїв, які не є комп'ютерами, не нова. Перший пристрій з підключенням до Інтернету був тостер з підтримкою протоколу IP, який можна було включати і вимикати через Інтернет, тостер був представлений на інтернет-конференції в 1990 році. Протягом наступних кількох років з'явилися інші предмети з підтримкою протоколу IP, включаючи автомат прохолодних напоїв в університеті Карнегі-Меллона в США і кавоварка в Троянському залі в Кембріджському університеті у Великій Британії, яка залишалася з підключенням до Інтернету до 2001 року. З найперших ексцентричних кроків наполеглива праця на ниві досліджень і розробок привела до створення «інтелектуальної мережі об'єктів», яка стала основою для сьогоднішнього Інтернету речей.

Надалі ми опишемо широкий спектр можливих областей застосування з точки зору умов, в яких IoT буде забезпечувати переваги для галузі і користувачів. Застосування технології Інтернету речей наводиться нижче в таблиці 1.1.

Таблиця 1.1 - Застосування технології Інтернету речей

Область	Приклади застосування
Людина (пристрої, закріплені на людському тілі або всередині нього)	Пристрої (носяться і проковтує) для моніторингу та підтримки здоров'я, а також для забезпечення гарного самопочуття людей; управління ходом захворювання
Точки роздрібних продажів (місця, де споживачі роблять покупки)	Магазини, банки, ресторани, будь-які місця, де люди приймають рішення про покупки, каси самообслуговування спеціальні пропозиції, оптимізація товарних запасів
Офіси (місця зайнятості працівників розумової праці)	Управління енергоспоживанням і безпекою в офісних будівлях; підвищення продуктивності, в тому числі, для мобільних співробітників
Виробничі підприємства (Виробниче середовище)	Місця з повторюваної послідовністю робочих операцій, включаючи лікарні і ферми; виробнича ефективність, оптимізація використання обладнання та інвентарю
Робочі об'єкти (спеціалізована виробниче середовище)	Гірська промисловість, нафтогазова промисловість, будівництво; виробнича ефективність, профілактичне обслуговування, здоров'я та безпеку
Транспортні засоби (системи всередині рухомих транспортних засобів)	Транспортні засоби, включаючи автомобілі, вантажівки, судна, літаки і поїзди; обслуговування за технічним станом, конструкція на основі умов використання
Міста (міське середовище)	Громадські місця і інфраструктура в міських умовах; адаптивне регулювання руху транспорту, інтелектуальні лічильники, моніторинг навколишнього середовища, управління ресурсами
Відкриті простору (за межами міського середовища та інших умов)	У число відкритих просторів входять залізничні колії, автономні транспортні засоби та аеронавігація; складання маршруту в реальному часі, послуги підключення навігації

1.2 Визначення терміна і концепції Інтернету речей

Сьогодні термін Інтернет речей широко використовується для опису сценаріїв, в яких підключення до Інтернету і обчислювальні функції поширюються на ряд різних об'єктів, такі як: персональні пристрої, датчики, прилади та інших предметів повсякденного жізні.Прежде ніж говорити про цей напрямок, необхідно з'ясувати, що таке

Інтернет речей і зрозуміти, чи існує визначення даного терміну. Втім, проблема не у відсутності визначень, а навпаки, в їх надлишку. Переглянувши кілька десятків іноземних статей і звітів на тему IoT, я переконався в наявності серйозних розбіжностей в трактуванні цього терміна. Для прикладу, наведу визначення з найбільш популярних і шанованих джерел.

Одна з найбільших китайських компаній в сфері телекомунікацій HuaweiTechnologies трактує поняття Інтернет речей, як набір технологій і додатків, якими обладнуються фізичні пристрої для підключення і отримання всіх видів інформації (місце розташування, температура, відсоток заряду), а також в залежності від отриманих даних, виполненять " розумні "дій.

Компанія Gartner дає определеніеІнтернета речей як мережу фізичних об'єктів, яка містять вбудовані технології для спілкування і взаємодії між собою для вимірювання стану зовнішнього середовища. Варто звернути увагу, що в обох визначеннях, найбільш часто цитований слово Internet взагалі відсутня. Тобто, кажучи про мережу Інтернет речей, не затверджується, що вона є частиною Інтернету. Більш того, відповідно до виразу, одного з фахівців по технології IoT Мета Трака (Matt Turck), керуючого директора компанії First Mark Capital, незважаючи на назву Інтернет речей, самі речі часто пов'язані з допомогою M2M протоколів, а не за допомогою Інтернету. Втім, наявність або відсутність підключення до Інтернету не єдина розбіжність у визначеннях.

Згідно з трактуванням міжнародної дослідницької компанії International Data Corporation (IDC) Інтернет речей - це дротова або бездротова мережа, що з'єднує пристрої, які мають вбудовані аналогові або цифрові датчики. Ці пристроїв мають автономне живлення і управляються програмним забезпеченням, розташованим на локальному сервері або віддаленому хмарі.

Компанія Cisco Business Solutions Group (CBSG) дає своє визначення, IoT - це стан Інтернету починаючи з моменту часу, коли кількість речей або об'єктів, підключених до всесвітньої мережі, перевищує населення планети. CBSG підкріплює свої висновки розрахунками. За даними компанії, вибухове зростання смартфонів і планшетних комп'ютерів довів число пристроїв, підключених до Інтернету, до 12,5 млрд в 2010 році, в той час як число людей, що живуть на Землі, збільшилася до 6,8 млрд; таким чином, кількість підключених пристроїв склало 1,84 одиниць на людину. Виходячи з цієї нескладної арифметики, Cisco Business Solutions Group фактично визначило саму точку настання ери Інтернету речей (рис. 1.1). Десь між 2003 і 2010 роком кількість підключених пристроїв перевищила населення планети, що й ознаменувало перехід в стан Інтернет

речей. При цьому автори дослідження вважають, що кількість підключених пристроїв на одну людину з числа інтернет-користувачів в 2010 році становило 6,25 штук.

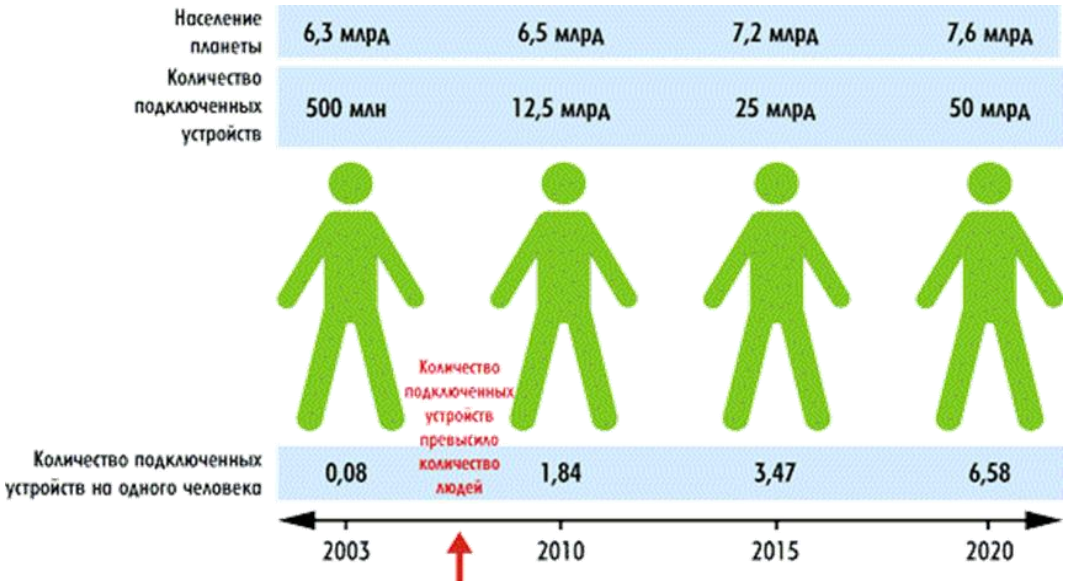


Рисунок 1.1 - Зростання числа підключених пристроїв на одну людину

Якщо Cisco згадує в зв'язку з терміном IoT про вибухове зростання смартфонів, підключених до Мережі, то IDC, наприклад, чітко говорить, що пристрої в концепції IoT повинні бути автономно підключені до Інтернету і передавати сигнали без участі людини. А тому смартфон, керований користувачами, до IoT-пристроїв віднесений бути не може.

Очевидно, що якщо аналітики оперують поняттям обсяг ринку IoT, то спиратися на настільки розпливчасте визначення, як якесь нове стан Інтернету, неможливо. При цьому про IoT, як про такий собі переході Інтернету в нову якість, говорять не тільки фахівці з CBSG. Обратімвніманіенарісунок 1.2, взятий із звіта Internet of Things (IoT) & Machine-To-Machine Communication Market. Він також характеризує IoT як етап у розвитку Інтернету, коли не тільки люди, а й речі починають взаємодіяти між собою, ініціювати транзакції, впливати один на одного.

Судячи з рисунка 1.2 Web 1.0 був статичний, HTML-сторінки переважно проглядалися користувачами при мінімальній інтерактивності. Web 2.0 був більш інтерактивним, дані циркулювали між користувачами і веб-сайтами, як, наприклад, в соціальних мережах (Facebook, Google+).

У Web 3.0 не тільки люди, а й речі починають взаємодіяти між собою, але вони також ініціюють транзакції і впливають один на одного.

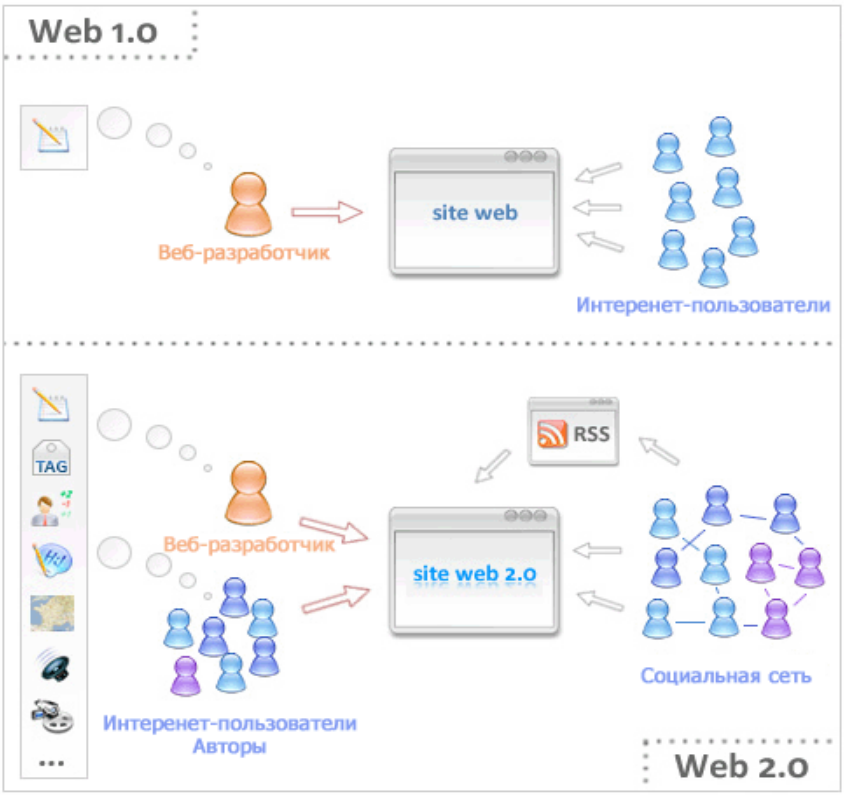


Рисунок 1.2 - Етапи розвитку Web 1.0 і Web 2.0

У цьому плані показовою є ще одна схема: ілюстрація зі статті корейського автора Sunsig Kim, опублікована в 2012 році. Тут стан IoT представляється як точка переходу - це наступний щабель, в порівнянні з технологією M2M (рис. 1.3). Навпаки, в публікаціях ряду авторів, включаючи IDC, можна прочитати, що M2M - це технологія, яка, будучи попередницею технології IoT, в даний час є її складовою частиною.

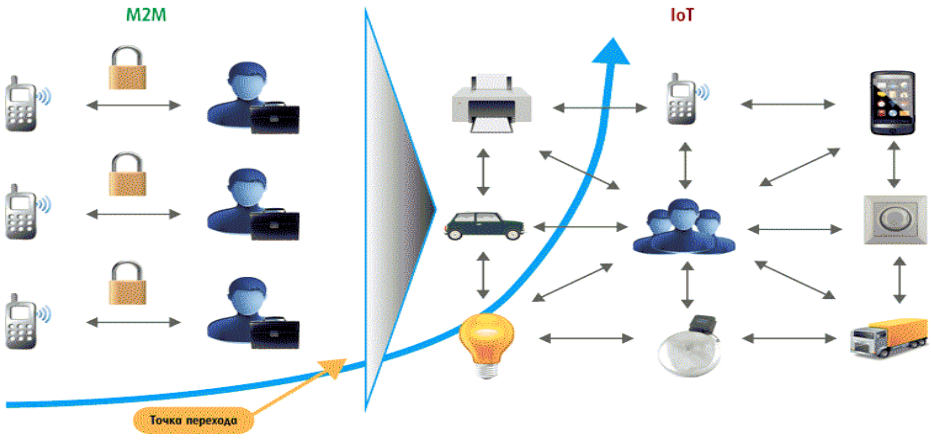


Рисунок 1.3 - Перехід від технологій M2M до технологій IoT

Якщо описані нами визначення говорять про що має місце явище, то, наприклад, в формулюванні Кайван Карімі (Kaivan Karimi), виконавчого директора по глобальній

стратегії і розвитку бізнесу Free scale Semiconductor, IoT - це швидше перспектива: мільярди розумних підключених речей, які формують свого роду універсальну глобальну нейронну мережу, яка буде включати всі аспекти нашої жізні. IoT складається з розумних машин, взаємодіючих і спілкуються з іншими машинами, об'єктами, навколишнім середовищем і інфраструктурою. У такій системі будуть генеруватися величезні обсяги даних, обробка яких може використовуватися для управління і контролю за речами, щоб зробити наше життя зручніше і безпечніше, а також знизити наше вплив на навколишнє середовище.

Чому ж так багато визначень, і всі вони різні?

По-перше, технології розвиваються так швидко, що постійно з'являється нове наповнення терміна, яке не завжди стикується з попередніми тлумаченнями. Це красномовно ілюструє рисунок 1.4, де еволюція IoT ототожнюється з декількома стадіями і, по суті, з різними технологіями.

Рисунок 1.4 - Еволюція технології Інтернет речей

По-друге, дуже часто нову технологію визначають, як сукупність чинників, що відрізняє її від попередньої, а потім таку попередню технологію включають в нове поняття. Рухомі маркетинговими устремліннями вендори хочуть старі технології називати новими іменами. Аналітики теж, слідуючи моді і прагнучи продемонструвати значимість

описуваного ринку, використовують один так званий зонтичний термін, поєднуючи в ньому кілька понять.

Аналогічна ситуація спостерігається і щодо інших нових термінів. Візьмемо, наприклад, термін SaaS, що виник для позначення наступному ступені розвитку технології ASP. Сьогодні в ряді публікацій ASP-проекти стали включати в ринок SaaS, що, строго кажучи, некоректно.

Приблизно те ж відбувається і з терміном IoT: з одного боку, це наступний щабель розвитку M2M-технологій, з іншого боку, у багатьох джерелах говориться, що ринок M2M-рішень є підмножиною IoT, а в деяких джерелах використовують абревіатуру IoT / M2M.

Ще одна причина неоднозначності терміну полягає в тому, що на базі IoT вирішуються різні класи задач. Зокрема, Кайван Карімі говорить про наявність, як мінімум, двох класів завдань, які об'єднує термін IoT. Перше завдання - це віддалений моніторинг і управління набором взаємопов'язаних мережевих пристроїв, кожне з яких може взаємодіяти з об'єктами інфраструктури та фізичної середовища. Наприклад, датчик температури і вологості контролює мережу приладів, які керують системою клімату розумного будинку (вікон, жалюзі, кондиціонерів та ін.). Більш екзотичний приклад - датчик на руці власника розумного будинку подає сигнал про психофізичному стані господаря всім розумним пристроїв, що знаходяться в мережі; кожне з них реагує певним чином, в результаті чого змінюється освітленість, фонова музика, кондиціювання. Тут основна функція НЕ аналітична, а саме керуюча.

Друге завдання - це використання даних, отриманих з кінцевих вузлів (смарт пристроїв з можливістю підключення і зондування) для інтелектуального аналізу з метою виявлення тенденцій і взаємозв'язків, які можуть генерувати корисну інформацію для забезпечення додаткової вигоди в бізнесі. Наприклад, відстеження поведінки відвідувачів у магазині за допомогою бирок на товарах: скільки часу і біля яких товарів зупиняються відвідувачі, які товари беруть в руки і т.п. На підставі цієї інформації можна змінити розташування товарів в залі і збільшити обсяг продажів.

Ще один приклад зі сфери автострахування. Розміщення в автомобілях пристроїв, забезпечених акселерометром, дозволить страховій компанії збирати дані про ступінь акуратності водіння клієнта. Фіксуватися можуть не тільки зіткнення, але і, наприклад, різкий наїзд на предмет або бордюр. Чим акуратніше водить клієнт, тим дешевше страховка, а лихач платить більше. В останніх прикладах не стоїть завдання управління, тут виконується збір даних і їх обробка методами сучасної аналітики. Статистична

інформація про всіх клієнтів дозволить компанії правильно прогнозувати свої ризики (рис. 1.6).

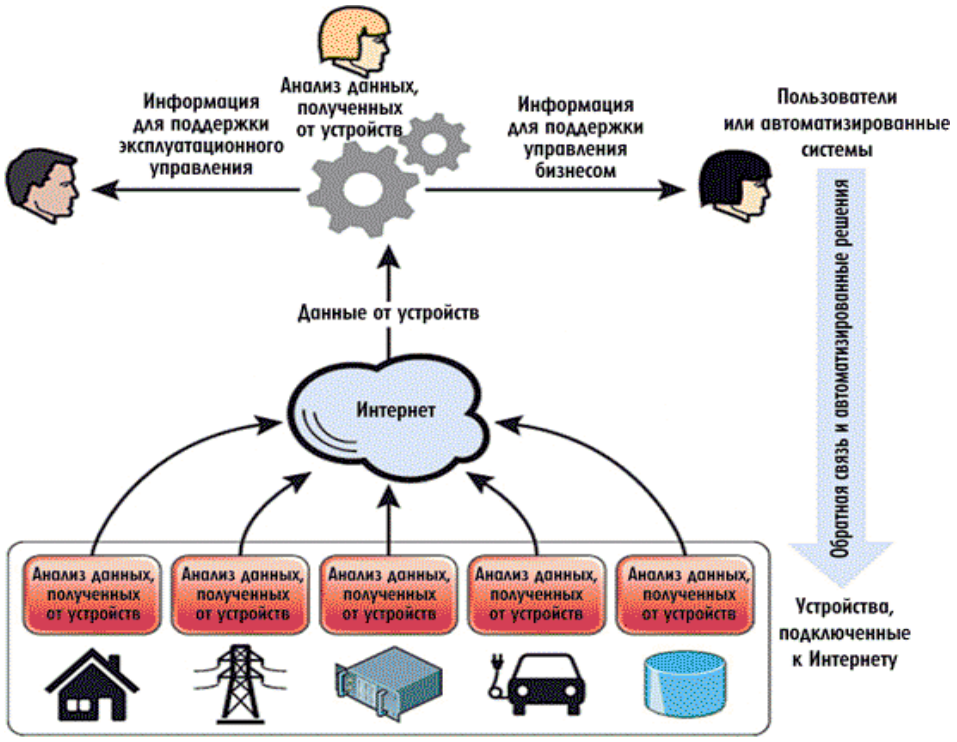


Рисунок 1.6 - Типова архітектура IoT-додатків

У своїх роботах Кайван Карімі представляє не тільки зображення типовий архітектури, але також графічну інтерпретацію всієї екосистеми Інтернету речей (рис. 1.7).

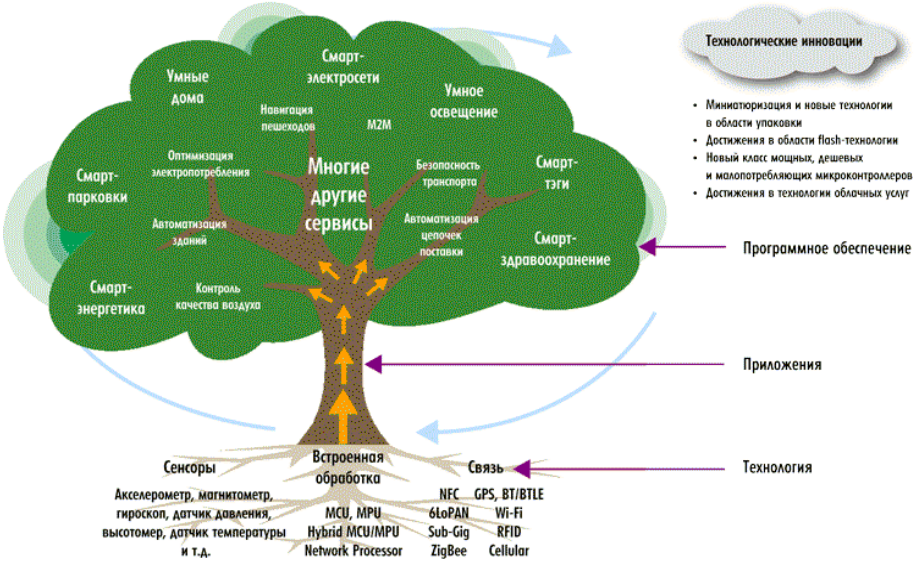


Рисунок 1.7 - Екосистема Інтернету речей

Всі надані вище визначення описують сценарії, в яких підключення до Інтернету і обчислювальні функції поширюються на ряд різних об'єктів, такі як: персональні пристрої, датчики, прилади та інших предметів повсякденного життя, які зазвичай не вважаються комп'ютерами. Ці пристрої можуть генерувати дані, а також обмінюватися ними з іншими пристроями в мережі при мінімальному втручанні з боку людини. Різні визначення Інтернету речей не завжди суперечать один одному, часто вони підкреслюють різні аспекти з різних точок зору і перспектив їх застосування. Однак різні визначення можуть стати джерелом плутанини і нерозуміння суті технології Інтернету речей, особливо при обговореннях між групами зацікавлених сторін або галузевими підприємствами. Можливо, створення єдиного визначення цієї технології і не потрібно, але в обговореннях необхідно враховувати різні точки зору.

Грунтуючись на вищеописаних визначеннях, хочеться підвести підсумок і виділити основну суть і базові принципи Інтернету речей, які будуть розглядатися і використовуватися в рамках цієї атестаційної роботи.

У загальному випадку під Інтернетом речей розуміється сукупність різних приладів, датчиків, пристроїв, об'єднаних в мережу за допомогою будь-яких доступних каналів зв'язку, що використовують різні протоколи взаємодії між собою і єдиний протокол доступу до глобальної мережі. У роботі в якості глобальної мережі дляІнтернет речей будемо використовувати мережу Інтернет. Спільним протоколом будетIP.

Під речами (things) ми будемо розуміти фізичні об'єкти (фізичні речі), які можуть бути ідентифіковані та об'єднані через комунікаційні мережі.

Інтернет речей грунтується на трьох базових принципах. По-перше, на повсюдно поширеною комунікаційної інфраструктури, по-друге, на глобальній ідентифікації кожного об'єкта і, по-третє, на можливості кожного об'єкта відправляти і отримувати дані за допомогою персональної мережі або мережі Інтернет, до якої він підключений.

1.3 Моделі комунікації в Інтернеті речей

З практичної точки зору корисно розглянути, як пристрої IoT здійснюють підключення та зв'язок у відповідності зі своїми технічними моделями зв'язку. У березні 2015 року комісія з архітектури Інтернет (IAB) випустила директивний документ по архітектурі для мережевого підключення інтелектуальних об'єктів, в якому визначається концептуальна основа чотирьох загальних моделей зв'язку, що використовуються пристроями IoT: від пристрою до пристрою, від пристрою до хмари, від пристрою до

шлюзу і модель спільного використання даних на сервері. Ця основа наводиться в обговоренні нижче з поясненням основних характеристик кожної моделі.

1.3.1 Підключення від пристрою до пристрою

Модель зв'язку від пристрою до пристрою являє два або кілька пристроїв, підключених і здійснюють зв'язок один з одним безпосередньо, а не через проміжний сервер додатків. Ці пристрої здійснюють зв'язок через різні типи мереж, в тому числі, мережі на основі протоколу IP або Інтернет. Однак часто ці пристрої використовують такі протоколи, як Bluetooth, Z-Wave або ZigBee для встановлення прямого зв'язку від пристрою до пристрою, як показано на рис. 1.8.

Рисунок 1.8 - Приклад моделі підключення від пристрою до пристрою

Ці мережі зі зв'язком від пристрою до пристрою дозволяють пристроїв, які підтримують певний протокол, здійснювати зв'язок і обмін повідомленнями для виконання своїх функцій. Ця модель зв'язку зазвичай застосовуються в таких додатках, як домашні системи автоматики, в яких зазвичай використовуються пакети даних малого розміру для встановлення зв'язку між пристроями з низьким рівнем вимог в області швидкості передачі даних. Побутові пристрої IoT, такі як лампочки, вимикачі, термостати і дверні замки, в домашній системі автоматики обмінюються малим обсягом інформації, наприклад, повідомлення про стан дверного замка або команда включення світла.

Цей зв'язок від пристрою до пристрою наочно демонструє багато проблем інтероперабельності, які будуть розглядатися нижче. Відповідно до опису в статті, опублікованій в IETF Journal, ці пристрої часто знаходяться в безпосередньому зв'язку,

зазвичай вони оснащені вбудованими механізмами безпеки, але також використовують певні моделі даних для кожного пристрою, що вимагають додаткових зусиль в розробці виробниками пристроїв. Це означає, що виробники пристроїв повинні вкладати кошти в розробку певних форматів даних для кожного типу пристроїв замість використання відкритої платформи для стандартних форматів.

З точки зору користувачів, це часто означає, що використовувані протоколи передачі даних від пристрою до пристрою несумісні, і в результаті користувач змушений вибирати інші пристрої, що підтримують той же протокол. Наприклад, пристрої, що використовують протокол Z-Wave, несумісні з пристроями сімейства ZigBee. Незважаючи на те, що ця несумісність обмежує вибір користувача пристроями, що належать до певного сімейства на основі одного і того ж протоколу, користувач знає, що продукти певного сімейства працюють належним чином.

1.3.2 Підключення від пристрою до хмари

У моделі зв'язку від пристрою до хмари пристрій IoT підключається безпосередньо до хмарної інтернет-службі, такий як постачальник послуг оренди додатків, для обміну даними та управління трафіком повідомлень. При такому підході часто використовуються існуючі механізми зв'язку, такі як традиційні дротяні з'єднання Ethernet або Wi-Fi для встановлення з'єднання між пристроєм і мережею IP, яка, в свою чергу, підключається до хмарної службі (рисунок 1.9).

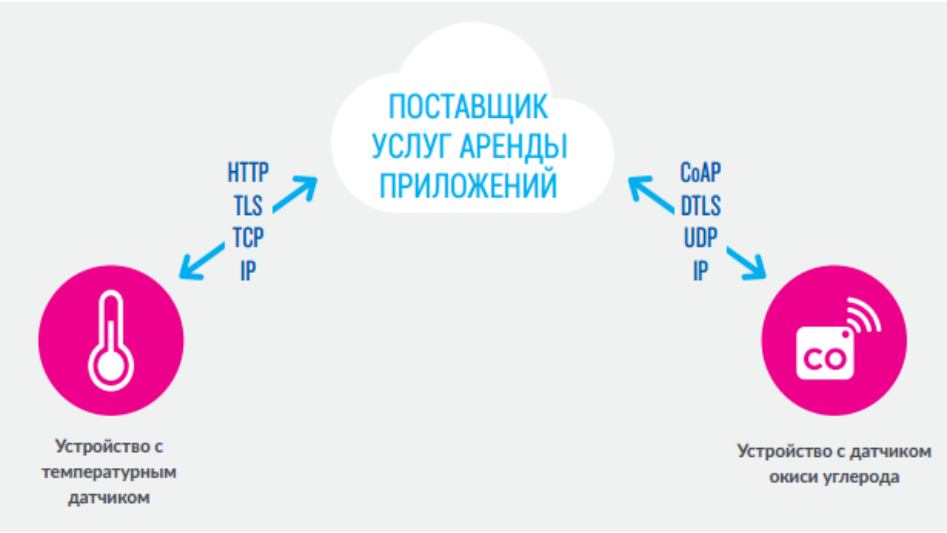


Рисунок 1.9 - Приклад моделі підключення від пристрою до хмари

Ця модель з'єднання використовується деякими популярними споживчими пристроями IoT, такими як самонавчальний термостат Nest Labs44 iSmartTV виробництва Samsung. У разі самонавчального термостата Nest пристрій передає дані в хмарну базу даних, де ці дані можуть використовуватися для аналізу споживання електроенергії вдома. Це хмарне підключення дозволяє користувачеві отримувати віддалений доступ до свого термостата через смартфон або веб-інтерфейс, а також підтримує оновлення програмного забезпечення термостата. Аналогічним чином, в разі технології SmartTV виробництва Samsung, телевізор використовує підключення до Інтернету для передачі інформації про переглядаються користувачем програмах в Samsung для аналізу і підключення інтерактивної функції розпізнавання голосу на пристрої телевізора. У цих випадках модель пристрій відобразився на хмарі забезпечує додаткову цінність для кінцевого користувача за рахунок розширення стандартних функцій пристрою.

Проте, проблеми інтероперабельності можуть виникнути при спробі інтеграції пристроїв різних виробників. Найчастіше використовуються хмарні послуги та влаштування одного виробника. Якщо для зв'язку між пристроєм і хмарними службами використовуються патентовані протоколи даних, власник або користувач пристрою може користуватися лише певною хмарної службою, що обмежує його можливість користуватися послугами інших постачальників. Така ситуація позначається терміном залежність від постачальника, яка охоплює різні аспекти відносин з постачальником, такі як володіння даними і доступ до них. У той же час користувачі зазвичай можуть бути впевнені в можливості інтеграції пристроїв, створених для певної платформи.

1.3.3 Підключення від пристрою і шлюзом

У разі моделі підключення між пристроєм і шлюзом або, найчастіше, в моделі підключення пристрою до шлюзу прикладного рівня (ALG) пристрій IoT підключається через службу ALG як канал для використання хмарної служби. Простіше кажучи, це означає, що прикладне програмне забезпечення функціонує на пристрої локального шлюзу, яке виконує роль посередника між пристроєм і хмарної службою і забезпечує безпеку і інші функції, такі як перетворення даних або протоколів (рис.1.10)

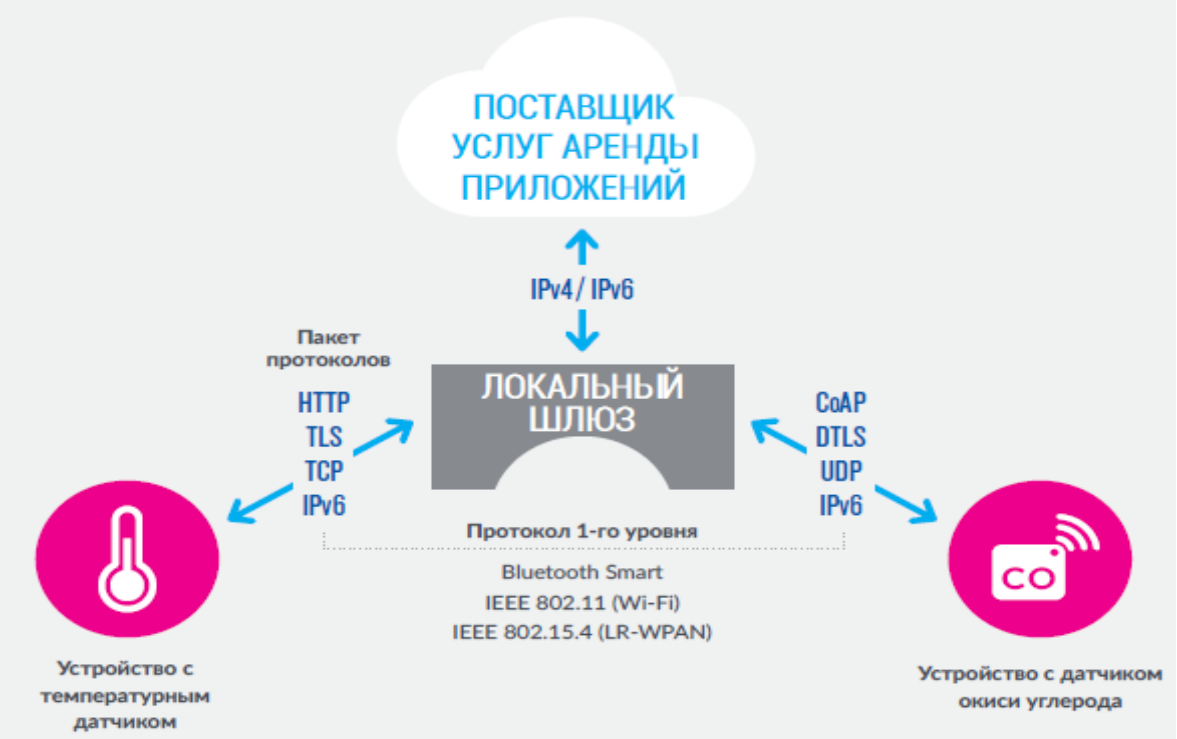


Рисунок 1.10 - Приклад моделі підключення від пристрою до шлюзу

У призначених для користувача пристроях присутні різні варіанти цієї моделі. У багатьох випадках в якості локального шлюзу використовується смартфон з додатком для зв'язку з пристроєм і передачі даних в хмарну службу. Ця модель часто використовується з популярними споживчими пристроями, такими як браслети для занять спортом. У цих пристроях відсутня функція прямого підключення до хмарної службі, тому вони часто використовують програми смартфона для роботи в якості шлюзу підключення.

Іншим різновидом цієї моделі підключення пристрою до шлюзу є пристрої, що виконують роль концентратора в додатках домашньої автоматики. Ці пристрої використовуються в якості локального шлюзу між окремими пристроями IoT і хмарної службою, але вони також можуть заповнювати прогалини інтероперабельності між самими пристроями. Наприклад, концентратор SmartThings є окремий пристрій шлюзу з трансиверами Z-Wave і Zigbee, встановленими для підтримки зв'язку з обома типами пристроїв. Це пристрій буде з'єднуватись з хмарної службою Smart Things, завдяки якому користувач може отримувати доступ до пристроїв за допомогою програми смартфона і підключення до Інтернету.

З більш широкої технічної перспективи, стаття в IETFJournal пояснює переваги використання моделі з'єднання пристрою зі шлюзом: ця модель зв'язку використовується в тих випадках, коли інтелектуальні об'єкти вимагають інтероперабельності з пристроями,

не підтримують протокол Інтернету IP. Іноді цей підхід використовується для інтеграції пристроїв, що підтримують тільки протокол IPv6, що означає, що шлюз необхідний для традиційних пристроїв і послуг, що підтримують тільки протокол IPv4.

Іншими словами, ця модель зв'язку часто використовується для інтеграції нових інтелектуальних пристроїв у традиційну систему з пристроями, які спочатку не можуть з ними взаємодіяти. Недолік цього підходу полягає в тому, що необхідність розробки системи і шлюзу прикладного рівня збільшує складність і вартість системи в цілому.

Очікується, що в майбутньому будуть створені більш універсальні шлюзи для зниження вартості та рівня складності інфраструктури для кінцевих споживачів, підприємств і промислового застосування. Існування таких універсальних шлюзів більш ймовірно в тому випадку, якщо пристрій розроблений таким чином IoT підтримує універсальні протоколи Інтернету і не вимагає наявності шлюзу прикладного рівня для перетворення протоколів. В цілому, використання шлюзів прикладного рівня призводить до більш нестійкого розгортання, як це спостерігалося в минулому.

Системи, що використовують модель з'єднання пристрою зі шлюзом, і їх роль у вирішенні проблем інтероперабельності пристроїв IoT досі перебувають в процесі розвитку.

1.3.4 Модель спільного використання даних на сервері

Модель спільного використання даних на сервері відповідає архітектурі, що дозволяє користувачам експортувати і аналізувати дані інтелектуальних об'єктів з хмарної служби в поєднанні з даними з інших джерел. Така архітектура підтримує бажання користувачів надавати доступ третім сторонам до завантаженим. даними датчиків. Такий підхід відповідає моделі з'єднання окремих пристроїв з хмарою, яка може привести до створення вихідної бази даних, де пристрої IoT завантажують дані тільки для одного постачальника послуг оренди додатків. Архітектура спільного використання даних на сервері дозволяє об'єднувати і аналізувати потоки даних, отриманих від одного пристрою Інтернету речей.

Наприклад, корпоративний користувач, відповідальний за офіс, може бути зацікавлений в об'єднанні і аналізі даних про фактичне споживання електроенергії та інших комунальних послуг, одержуваних усіма датчиками IoT і системами інженерного забезпечення з підключенням до Інтернету. У моделі підключення окремих пристроїв до хмарним службам дані кожного датчика або системи IoT знаходяться в окремій базі

даних. Ефективна архітектура спільного використання даних на сервері повинна дозволяти компанії з легкістю отримувати доступ і аналізувати хмарні дані, отримані від всіх пристроїв в будівлі. Крім того, цей тип архітектури дозволяє забезпечити переносимість даних. Ефективна архітектура спільного використання даних на сервері дозволяє користувачам переміщати свої дані при перемиканні між послугами IoT, долаючи бар'єри традиційних роздільних баз даних.

Модель спільного використання даних на сервері передбачає об'єднаний підхід до хмарним послуг; в іншому випадку необхідні хмарні інтерфейси прикладного програмування (API) для забезпечення інтероперабельності розміщених на хмарі даних з інтелектуальних пристроїв (рис. 1.11).

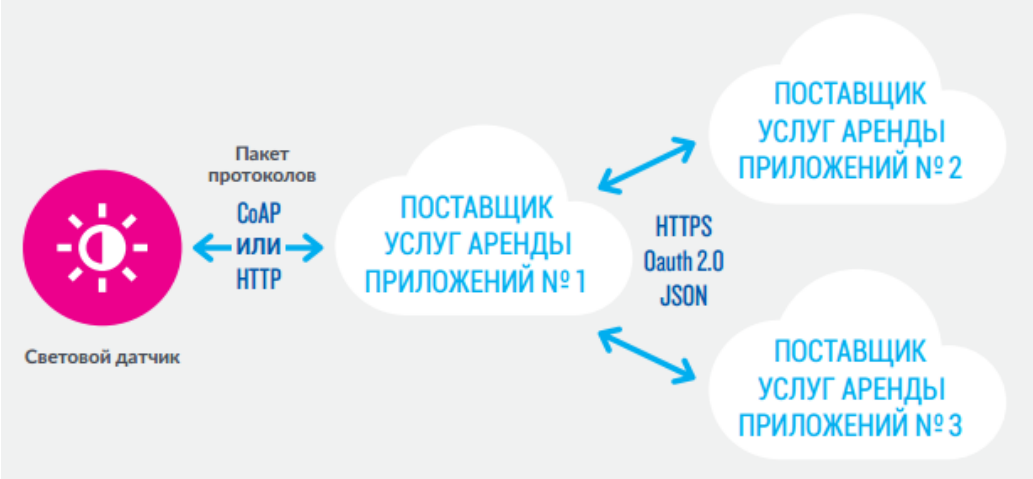


Рисунок 1.11 - Модель спільного використання даних на сервері

Дана модель архітектури є підхід для забезпечення інтероперабельності між цими системами на базі сервера. Як вказується в IETFJournal, стандартні протоколи можуть полегшити завдання, але їх недостатньо для видалення вузькоспеціальних баз даних, так як для взаємодії між різними виробниками необхідна наявність загальних інформаційних моделей. Іншими словами, ця модель зв'язку ефективна тільки на основі архітектури системи IoT. Архітектура на основі загального використання даних на сервері не може в повній мірі компенсувати закриту конструкцію системи.

Чотири основні моделі зв'язку демонструють стратегії розробки, що застосовуються для забезпечення зв'язку між пристроями IoT. Крім технічних аспектів, застосування цих моделей багато в чому визначається відмінностями між патентованими і відкритими пристроями IoT в мережі. А в разі використання моделі зв'язку пристрою зі шлюзом її основною характеристикою є її здатність подолання обмежень при підключенні

патентованих пристроїв IoT. Це означає, що интероперабельность пристроїв і відкриті стандарти є ключовою умовою для створення і розвитку взаємопов'язаних систем IoT.

Ці моделі зв'язку дозволяють краще зрозуміти можливість створення додаткової цінності для кінцевих користувачів за допомогою мережевих пристроїв. Загальна цінність пристроїв підвищується за рахунок надання користувачам більш зручного доступу до пристроїв IoT і їх даними. Наприклад, в трьох з чотирьох моделей зв'язку пристрої підключаються до служб аналізу даних на основі хмарних обчислень. За рахунок створення каналів передачі даних на хмару користувачі і постачальники послуг можуть більш швидко і легко об'єднувати дані, проводити їх великий аналіз і візуалізацію, а також застосовувати технології аналітичного прогнозування, щоб скористатися додатковими перевагами даних IoT, одержуваних за допомогою традиційних додатків вузькоспеціальних баз даних. Іншими словами, ефективні моделі зв'язку є важливим фактором для підвищення цінності послуг для кінцевих користувачів за рахунок можливості застосування нових способів використання інформації. Однак, незважаючи на ці переваги, тут також є недоліки. При виборі архітектури необхідно ретельно врахувати питання додаткових витрат для користувачів при підключенні до хмарним ресурсів, особливо в регіонах з високою вартістю послуг зв'язку.

Незважаючи на переваги ефективних систем зв'язку для користувачів, слід зауважити, що ефективні моделі зв'язку IoT також сприяють розвитку технічних інновацій і відкривають можливості комерційного зростання. Для того, щоб скористатися перевагами раніше не існували потоків даних IoT, можуть створюватися нові продукти і послуги, які виконують роль каталізатора для подальших інновацій.

Представлені вище моделі зв'язку демонструють стратегії розробки, що застосовуються для забезпечення зв'язку між пристроями Інтернету речей, однак не можна сказати, як модель універсальна або яка використовується частіше, все залежить від того що ви хочете отримати в кінцевому підсумку і які вимоги пред'являються мережі, вибір залишається за вами.

1.4 Організація дротового і бездротового зв'язку в Інтернеті речей

У промишленномIoT основними різновидами речей, які треба підключати до мережі, є різні типи датчиків (сенсорів) і приводів. Ці пристрої з одного боку мають інтерфейс з комунікаційною мережею, а з іншого, інтерфейс, що забезпечує фізичне взаємодія з процесом, який потрібно відстежувати. Завдання датчиків і сенсорів -сбор

інформації. Вони можуть фіксувати різні фізичні характеристики (температуру і вологість, напруга і силу струму, витрата газу і рівень рідини), присутність різних речовин (хімічні та біосенсори), а також фізичні події, наприклад, зміна і переміщення об'єктів. Сенсори все частіше інтегруються безпосередньо в мікросхеми.

Крім сенсорів, в мікросхеми можуть вбудовуватися і приводи, призначення яких - контроль за фізичними об'єктами і управління ними. Такі інтегровані рішення називають мікро електромеханічними системами (МЕМС). Прикладами подібних пристроїв, що поєднують в собі мікроелектронні і мікромеханічні компоненти, є акселерометри і гіроскопи. Класичні ж приклади приводів - це мотори, що переміщують різні об'єкти; клапани, що відкривають та закривають канали надходження рідини або газу; електричні перемикачі. Приводи зазвичай мають механічний, гідравлічний, пневматичний або електричний компонент для виконання необхідних функцій, а також електронний блок управління. Комунікаційний інтерфейс - необхідний компонент пристрою IoT. Це може бути провідний або бездротової інтерфейс.

1.4.1 Технології дротового підключення

Основним кандидатом на універсальну технологію дротового зв'язку є Ethernet. У разі бездротового підключення це може бути Wi-Fi, а також безліч інших технологій. Але, незалежно від того, яка технологія використовується на канальному і фізичному рівнях, пристрій повинен безпосередньо підтримувати протокол IP, щоб інтегруватися в інфраструктуру IoT. Крім того, найважливішою умовою використання пристрою IoT є наявність засобів безпеки. IP - це відкритий протокол, тому такі кошти повинні бути інтегровані в пристрій спочатку.

Незважаючи на розбіжності в цифрах, більшість фахівців в області технологій сходяться на думці, що до 2025 року до мережі Інтернет будуть підключені мільярди додаткових пристроїв, від промислових датчиків до побутової техніки та автомобілів. У міру розвитку Інтернету речей пристрої, для яких потрібно наскрізне Інтернет-з'єднання, не зможуть використовувати протокол IPv4, застосовуваний зараз більшістю інтернет-служб. Для цього буде потрібно нова технологія IPv6.

IPv6 - це довгоочікуване оновлення основного вихідного протоколу IP, який підтримує всі з'єднання через Інтернет. Протокол IPv6 необхідний у зв'язку з тим, що в Інтернета закінчуються унікальні адреси IPv4. Незважаючи на те, що протокол IPv4 може підтримувати 4,3 млрд підключених до Інтернету пристроїв, IPv6 з адресами в кількості 2

в 128-го ступеня невичерпний для практичного застосування. Це більш ніж достатньо, щоб задовольнити потрібності пріблізітельно 100 млрд пристроїв IoT, які будуть введені в експлуатацію в найближчі десятиліття.

З урахуванням прогнозованого тривалого терміну служби деяких датчиків і інших пристроїв, призначених для Інтернету, проектні рішення будуть впливати на зручність цих рішень протягом десятиліть. Основною складністю для розробників IoT є те, що протокол IPv6 з самого початку не інтероперабелен з IPv4, і велика частина недорогого програмного забезпечення для вбудовування в пристрої IoT використовує тільки протокол IPv4. Проте, багато фахівців вважають, що IPv6 - це найкращий варіант зв'язку, який дозволить IoT повністю розкрити свої можливості.

Традиційно в промислових мережах переважна більшість підключень були провідними. Однак останнім часом бездротові технології використовуються все ширше. Найчастіше їх застосовують для некритичних додатків, таких як конфігурація і моніторинг, передача додаткових даних, підтримка додатків мобільних співробітників.

Однією з складних проблем застосування радіо-технологій є колективна середовище передачі (використання загального частотного діапазону), що може привести до неможливості передачі даних, якщо все частотні канали виявляться зайнятими. Крім того, радіозв'язок схильна до негативного впливу електромагнітних завад, які в виробничих цехах можуть бути досить істотними. Випадкова втрата пакетів також досить типова для багатьох радіосистем. Якщо для офісних мереж це прийнятно, то для критично важливих промислових рішень потрібна передача даних без втрат.

Одним із напрямів удосконалення радіо-технологій з метою їх застосування на виробництві є розробка ефективних технологій захисту від статичної електрики. За допомогою бездротової мережі з комірчастою топологією дозволяє знизити затримку і час реконфігурації мережі, а алгоритмів паралельної передачі - виключити втрати пакетів. У мережах розумних фабрик майбутнього бездротові технології будуть використовуватися досить широко, хоча основу, як і раніше, складуть провідні рішення.

Мережі Промислового інтернету речей за визначенням не можуть бути обмежені периметром того чи іншого підприємства. Важливе значення мають взаємодія з виробленим продуктом на етапі його експлуатації, а також доступ до хмарних сервісів, які можуть бути розкиданих по всьому світу. Тому територіально розподілена інфраструктура - ключева характеристика промислового інтернету.

1.4.2 Бездротові технології підключення

Якщо говорити про бездротових технологіях, на даний момент для підключення речей до Інтернету найбільш активно використовуються мережі стільникового зв'язку. Причому розвиток останніх в рамках організації 3GPP йде саме в напрямку адаптації до потреб IoT. В рамках розробки систем покоління 5G зміна структури кадру дозволить на порядок скоротити затримку (в порівнянні з системами LTE) до 1 мс. Крім того, спеціальні рішення розробляються для інтернету низької підключення великої кількості пристроїв при збільшеною зоні покриття.

Але, оскільки наявні технології стільникового зв'язку створювалися для обслуговування людей, а не речей, вони погано адаптовані для IoT (висока вартість, проблеми з покриттям та ін.). Тому активно розвиваються і альтернативні бездротові технології, в тому числі для розподілених мереж з низьким енергоспоживанням Wi-Fi, ZigBee iBluetooth, які будуть працювати на частотах загального пользованія.На малюнку 1.12 представлені основні бездротові технології, які використовуються в IoT, а також їх характеристики.

Технология	Назначение	Базовые характеристики	Организация, занимающаяся стандартизацией и/или продвижением
Bluetooth Low Energy	Персональные сети (PAN)	Низкая пропускная способность, малое энергопотребление	Bluetooth Special Interest Group
Wi-Fi	Локальные сети	Высокая пропускная способность, высокое энергопотребление	IEEE
ZigBee	Локальные сети	Низкая пропускная способность, малое энергопотребление	IEEE
GSM, GPRS, EC-GSM-IoT (EC — Enhanced Coverage)	Территориально распределенные сети (WAN), глобальное покрытие	Недорогие сотовые модемы, низкая пропускная способность	3GPP
HSPA	WAN, глобальное покрытие	Недорогие сотовые модемы, высокая пропускная способность, высокое энергопотребление	3GPP
LTE, NB-IoT	WAN, глобальное покрытие	Широкий диапазон скоростей, снижение стоимости и энерго-потребления в будущих релизах 3GPP	3GPP
«Стриж»	Территориально распре-деленные сети с низким энергопотреблением (LPWAN)	Низкая пропускная способность, малое энергопотребление, нелицензируемый диапазон (868 МГц)	Компания «Стриж»
LoRa	LPWAN	Низкая пропускная способность, малое энергопотребление, нелицензируемый диапазон	LoRa Alliance
Sigfox	LPWAN	Низкая пропускная способность, малое энергопотребление, нелицензируемый диапазон	Sigfox

Рисунок 1.12 - Деякі бездротові технології для IoT

Бездротові мережі можуть бути також класифіковані за їх топології як вузли мережі розташовані і з'єднані один з одним. Перші дві фундаментальні мережеві топології - це зірка і меш, які наочно показані на малюнку 1.13.

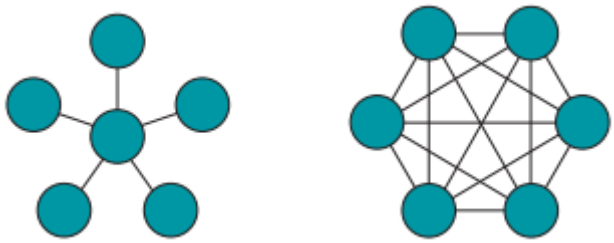


Рисунок 1.13 - Топологія зірка (зліва) і меш топологія (праворуч)

У топології зірка, всі вузли підключені до одного центрального вузла, який, як правило, також використовується в якості шлюзу для доступу в Інтернет. Популярним прикладом топології зірка є мережа Wi-Fi, де центр - це вузол, який називається точкою доступу (AP) та інші вузли називаються станціями.

У комірчастої мережі (меш), кожен вузол може підключатися до кількох інших вузлів. Один або кілька вузлів у мережі служать в якості Інтернет-шлюзу. У прикладі показано, що кожен вузол мережі з'єднаний з кожним іншим вузлом. У реальному житті топологія мережі простіше. Популярний приклад комірчастої мережі являє собою мережу Zig Bee Light Link, де кілька вузлів утворюють порожнисту мережу для розширення охоплення мережі у великих будинках. Один з Zig Bee вузлів називається координатор, і це, як правило, служить також як інтернет-шлюзу. Проте, ніздрюваті мережі є більш складними для розробки і можуть демонструвати більш тривалу затримку маршрутизації повідомлення від віддаленого вузла через сітку, в порівнянні з зіркоподібними мережами. Перевагою меш мережі є те, що він може розширити діапазон мережі, зберігаючи при цьому низьку потужність передачі радіосигналів. Максимальна кількість одночасно підключаються, також є важливим фактором при проектуванні системи. Деякі технології, такі як Bluetooth поддержіваютдо 20 з'єднань, в той час як Zig Bee, може підтримувати тисячі підключень.

До сих пір ми розглянули деякі з ключових концепцій в області бездротового зв'язку і обговорили інженерні компроміси в проектуванні бездротової системи зв'язку. Далі ми розглянемо домінуючі технології бездротового підключення в галузі і їх застосування більш докладно.

Технологія Wi-Fi, заснована на стандарті IEEE 802.11, була розроблена в якості бездротового заміни для популярного проводового стандарту IEEE 802.3 Ethernet.

Названіе Wi-Fi походить від скорочення словосполучення Wireless Fidelity (точна бездротовий зв'язок) і є стандартом зв'язку пристроїв в бездротової мережі (WLAN).

Підключення Wi-Fi часто є очевидним вибором для багатьох розробників, особливо з огляду на поширеність Wi-Fi в домашніх умовах і в локальних мережах. Крім того, Wi-Fi основан на топології зірка. Зв'язок йде від бездротових вузлів (пристроїв) до бездротової точки доступу (маршрутизатор або мережевий контролер).

В даний час іспользуетсястандарт 802.11ac, який був випущений в 2013 році, хоча версія стандарту 802.11n, який був випущений в 2009 році, як і раніше широко поширені. 802.11ac забезпечує швидкість до 800Mbit / с, тоді як 802.11n надає до 150Mbits / с.Ви можете також бачили пристрої, які мають навіть більш старі стандарти 802.11a / B / G, які тепер називаються застарілими. Однак, так як Wi-Fi має сумісність зверху вниз, старі пристрої продовжують працювати з пристроями, що мають нові стандарти.

Діапазон роботи WiFi пристрою залежить від декількох факторів: перше, це якийсь Wi-Fi стандарт працює на пристрої і друге, це наявність фізичних перешкод, наприклад, стіни також відіграють вирішальну роль у визначенні діапазону. Таким чином, у відкритих просторах діапазон мережі Wi-Fi буде більше, ніж в закритих приміщеннях зі стінами і іншими інтерферируючими об'єктами. Наочне зображення WiFi мережі підключення представлено на рисунку 1.14.

Рисунок 1.14 - Приклад використання Wi-Fi мережі

Bluetooth технологія була названа в чес ть стародавнього скандинавського короля ГаральдаБлютуса (Harald Bluetooth), який увійшов в історію як збирач земель скандинавських. Зокрема, йому приписується об'єднання Данії і Норвегії, а технологія Bluetooth мала об'єднати телекомунікаційну та комп'ютерну індустрію. Технологія була винайдена компанією Ericsson в 1994 році в якості стандарту для бездротового зв'язку між

телефонами і комп'ютерами. Канальний рівень Bluetooth, що працює в ISM-діапазоні 2,4 ГГц, що не був раніше стандартизований як стандарт IEEE 802.15.1, але в даний час стандарт IEEE більше не підтримується і стандарт Bluetooth управляється BluetoothSIG. Bluetooth став настільки успішним, що всі мобільні телефони сьогодні, навіть початкового рівня, мають можливість з'єднання Bluetooth. Основний варіант використання, який зробив Bluetooth популярним спочатку билабеспроводная зв'язок телефону і гарнітури. Bluetooth є технологією PAN і в основному використовується сьогодні в якості заміни кабелю для короткодіючого зв'язку. Технологія досить низько енергоспоживаюче, пристрої зазвичай використовують невеликі акумуляторні батареї або дві лужні батареї.

При розробці Bluetooth також враховувалося забезпечення стійкості до перешкод від Wi-Fi пристроїв, із застосуванням алгоритму стрибкоподібної перебудови частоти, щоб повідомлення Bluetooth пристроїв могли передаватися навіть при одночасній активності в декількох каналах Wi-Fi. Нарешті, в силу дуже малої потужності свого передавача зв'язок по Bluetooth менше схильна до впливу багатопроменевого поширення, в порівнянні зі зв'язком по Wi-Fi. Завдяки цьому для застосування Bluetooth не потрібно глибоке вивчення і планування радіо-обстановки в місці експлуатації. Система дуже стійка до впливу сторонніх і взаємних перешкод.

Перевагою Bluetooth є діапазон його роботи від 10 м до 100 м, однак це ж і є його недоліком, при великих потужностях передачіна великі дистанції необхідно більш високе споживання енергії.

ZigBee - наібільш часто використовуваний протокол для бездротових сенсорних мереж. ZigBee - це по суті не окремий протокол, а специфікація мережевих протоколів верхнього рівня (рівня додатків і мережевого рівня), що використовують сервіси нижніх рівнів: рівня управління доступом до середовища і фізичного рівня, регламентованих стандартом IEEE 802.15.4. ZigBee і IEEE 802.15.4 описують бездротові персональні обчислювальні мережі (WPAN). Специфікація ZigBee орієнтована на програми, що вимагають гарантованої безпечної передачі даних при відносно невеликих швидкостях і можливості тривалої роботи мережевих пристроїв від автономних джерел живлення (батарей).

Основна особливість технології ZigBee полягає в тому, що вона при малому енергоспоживанні підтримує не тільки прості топології мережі (точка-точка і зірка), але і самоорганізується і самовідновлюється порожнисту (mesh) топологію (рис. 1.15) з ретрансляцією і маршрутизацією повідомлень. Крім того, специфікація ZigBee містить можливість вибору алгоритму маршрутизації, в залежності від вимог програми та стану мережі, механізм стандартизації додатків - профілі додатків, бібліотека стандартних

кластерів, кінцеві точки, прив'язки, гнучкий механізм безпеки, а також забезпечує простоту розгортання, обслуговування та модернізації.

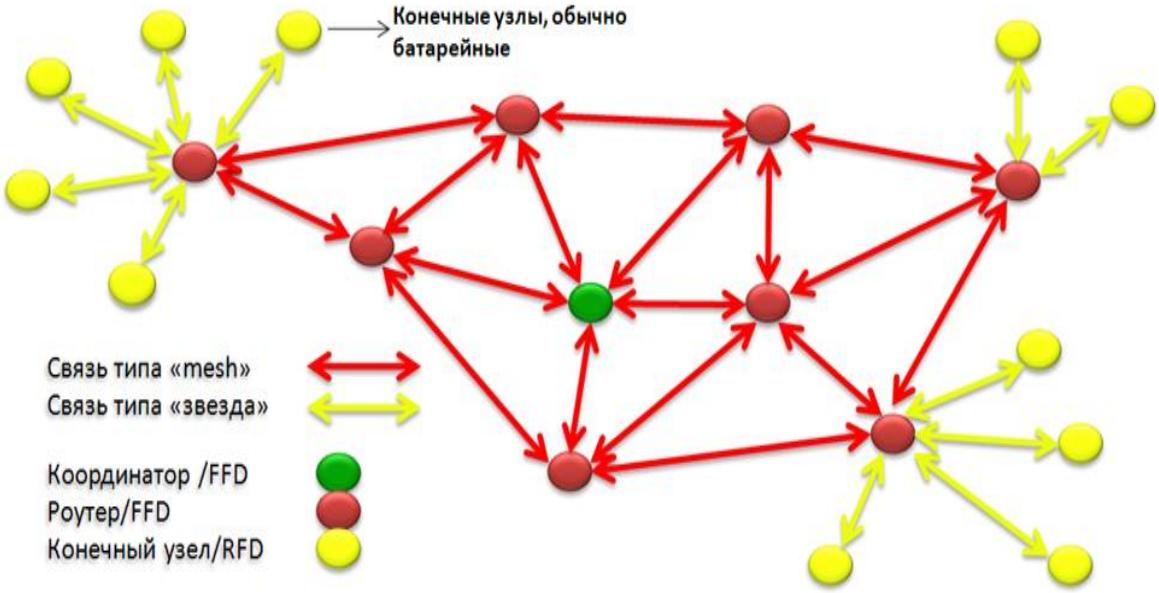


Рисунок 1.15 – Самовосстанавливающаяся ячеистая (mesh) топология

Як вже говорилося, кількість підключених пристроїв з кожним роком зростає все більше і більше. Обсяги зібраних даних також кардинально збільшуються. Тому необхідні технічні рішення, здатні забезпечити підключення великої кількості різних пристроїв просто і ефективно, при виконанні вимог до продуктивності, безпеки і надійності. На думку більшості експертів, домінуючі в минулому шини поступляться місцем універсальним мереж Ethernet. Для безшовної зв'язку як між елементами в рамках одного підприємства, так і з об'єктами зовнішнього світу будуть використовуватися стандартні інтернет-протоколи, тому і говорять про промислове інтернеті.

Адаптація традиційних мережевих рішень до вимог промислового інтернету йде по декількох напрямках. Одна з тенденцій спрощення кабельної системи. Типові системи Gigabit Ethernet задіють усі чотири пари провідників медножільной СКС. Однак уже розроблений стандарт Ethernet (1000Base-T1) для передачі гигабитного трафіку по одній парі - правда, з деякими обмеженнями по відстані. Системи FastEthernet також можуть працювати по одній парі, причому при стандартній дальності.

Інший важливий момент, що не залежить від того, використовується дротова або бездротова зв'язок - це зниження розмірів пристроїв і скорочення енергоспоживання. Прогрес в області напівпровідникової техніки дозволяє виробляти все більш компактні

структури, забезпечувати більш високу ступінь інтеграції та скорочувати енергоспоживання. Так, системи Wi-Fi з низьким споживанням можуть використовуватися для підключення невеликих датчиків, які отримують живлення від вбудованих акумуляторних батарей. Радіо технологій з низьким енергоспоживанням багато, але використання Wi-Fi дозволяє побудувати однорідну мережеву інфраструктуру, в якій кадри Ethernet і протокол IP будуть застосовуватися з кінця в кінець.

Для багатьох застосувань в промисловості необхідна гарантована затримка при передачі даних. Причому такі гарантії можуть знадобитися не тільки при зв'язку об'єктів в межах виробничої зони або підприємства, а й при взаємодії з об'єктами поза підприємства. В даний час існує ряд протоколів реального часу, які здатні забезпечити жорсткі гарантії по затримці в мережі Ethernet. Але жоден з цих протоколів не є стандартом Ethernet.

Для роботи в режимі реального часу можуть використовуватися різні технології, наприклад, протокол Precision Time Protocol (PTP), який забезпечує синхронізацію годин, вбудованих в мережеві пристрої. Цей протокол вже активно застосовується в багатьох мережах. Організація IEEE постійно працює над вдосконаленням PTP, в 2016 році повинен бути прийнятий стандарт вже на третю версію цього протоколу. Досягненню стабільної низької затримки сприяють також підвищення пропускної здатності каналів зв'язку і застосування алгоритмів пріоритезації трафіку всередині комутаторів. Очевидно, що чим ширша смуга пропускання доступна, тим нижча ймовірність того, що комутатор блокує той чи інший пакет.

Зі збільшенням числа підключених до мережі пристроїв і підвищенням значущості її безперебійної роботи кардинально змінюються вимоги до її адміністрування та експлуатації. До сих пір величезний обсяг пов'язаних з мережами робіт виконується вручну. Проектування мережі, інсталяція обладнання, його конфігурація, тестування, моніторинг роботи, технічне обслуговування, пошук та усунення несправностей - все це вимагає величезних людських і фінансових ресурсів. У майбутніх мережах IoT частка ручної праці повинна істотно скоротитися. Це необхідно, зокрема тому, що при збільшенні числа підключених пристроїв в сотні і тисячі разів стане фізично неможливо, наприклад, налаштовувати кожне окреме пристрій.

Обмежений обсяг статті не дозволяє детально розглянути всі аспекти, пов'язані з розвитком технології IoT. Зазначу, що ключове значення мають питання забезпечення безпеки таких рішень. Відмовостійкість мереж -також надзвичайно важливий аспект. Жорсткі умови експлуатації підвищують ймовірність пошкодження тих чи інших елементів мережевих структур, при цьому наслідки простою промислової мережі можуть мати величезний негативний ефект. У деяких випадках такий простий взагалі

неприпустимий, тому що може привести до катастроф і масової загибелі людей. На даний момент існує чимало механізмів, що забезпечують гаряче резервування мережевих елементів і гарантують продовження роботи навіть у разі пошкодження частини вузлів і каналів зв'язку. Такі механізми активно розвиваються і мають обов'язково використовуватися в промислових мережах.

1.5 Ключові проблеми Інтернета речей

Перед Інтернетом речей варто ряд проблем, які можуть перешкодити нам скористатися його потенційними перевагами. Постійні повідомлення про злом підключених до Інтернету пристроїв, проблеми ведення спостереження і побоювання щодо особистої конфіденційності вже привернули увагу громадськості. На даний момент технічні питання продовжують залишатися невирішеними, а також виникають нові складності в області політики, законодавства та подальшого розвитку.

Були вивчено три ключові області проблем IoT для визначення найбільш нагальних проблем і питань, пов'язаних з цією технологією. Ці області включають безпеку, конфіденційність, а також інтероперабельність і стандарти.

1.5.1 Забезпечення безпеки Інтернету речей

Забезпечення безпеки, надійності, стійкості і стабільності додатків і послуг Інтернету, має критично важливе значеніедля доверіяі використання Інтернету. Як користувачі Інтернету, ми повинні мати високий ступінь впевненості в тому, що Інтернет, його програми та підключені до нього пристрої мають досить високий ступінь безпеки для виконання різних завдань по відношенню до допустимості ризику, пов'язаного з їх виконанням. Інтернет речей нічим не відрізняється в цьому відношенні, і безпеку IoT пов'язана, в основному, з довірою до середовища з боку користувачів. Якщо люди не вірять в захищеність підключених пристроїв і отриманої інформації від неприпустимого використання, цей недолік довіри призводить до відмови від використання Інтернету. Цей фактор робить глобальний вплив на електронну комерцію, технічні інновації, свободу висловлювань і практично всі інші аспекти діяльності онлайн. Забезпечення безпеки продуктів і послуг IoT має бути основним пріоритетом в даній галузі.

У міру постійного збільшення числа пристроїв, підключених до Інтернету, виникають нові потенційні вразливі місця. Недостатньо захищені пристрої можуть служити точками доступу для кібератак, дозволяючи зловмисникам перепрограмувати пристрій або викликати його несправність. Пристрої недосконалою конструкції можуть піддавати дані користувачів небезпеки розкрадання за рахунок недостатній захист потоків даних. Несправні або дефектні пристрої також можуть створювати вразливі точки. Для поширених недорогих пристроїв невеликого розміру ці проблеми стоять настільки ж гостро або навіть ще гостріше, ніж для комп'ютерів, які традиційно використовувалися для підключення до Інтернету. Конкурентоспроможна вартість і технічні обмеження пристроїв IoT змушують виробників вбудовувати в ці пристрої відповідні функції безпеки, щоб забезпечити рівень безпеки і довгострокової захисту вразливих місць, що перевищує аналогічні показники комп'ютерів.

Крім потенційних вразливих місць, суттєве збільшення кількості і типів пристроїв IoT також може сприяти збільшенню ймовірності кібератак. З урахуванням функції взаємопідключення пристроїв IoT, кожне підключений пристрій, що не має достатнього захисту, надає потенційно негативний вплив на безпеку і стійкість Інтернету вглобальном масштабі, а не тільки локально. Наприклад, незахищений холодильник в США, заражений шкідливим програмним забезпеченням, може відправляти тисячі шкідливих повідомлень електронної пошти одержувачам у всьому світі за допомогою домашнього підключення Wi-Fi.

І на довершення всього, в гіперпідключених світі наша здатність виконувати щоденні завдання без допомоги пристроїв або систем з підключенням до Інтернету, буде знижуватися. Зараз стає все важче придбати пристрої без підключення до Інтернету, тому що деякі виробники виготовляють тільки підключення продукти. Кожен день ступінь нашої підключеності зростає, і ми стаємо все більш залежними від пристроїв IoT для виконання основних завдань. Необхідно, щоб пристрої були захищеними, з урахуванням того, що ніяке пристрій не може бути повністю безпечним. Цей зростаючий рівень залежності від пристроїв IoT і інтернет-послуг, з якими вони взаємодіють, також відкриває зловмисникам можливості доступу до пристроїв. Припустимо, ми можемо відключити підключений до Інтернету телевізор, якщо він піддасться кібератаці, але ми не зможемо також просто вимкнути електролічильник або систему регулювання руху транспорту або імплантований кардіостимулятор.

Саме тому безпека пристроїв і послуг IoT є основою темою обговорень і повинна бути визнана критично важливою проблемою. Ми все більшою мірою залежимо від цих

пристроїв для виконання важливих повсякденних завдань, і їх поведінка може надавати глобальний вплив.

1.5.2. Дотримання конфіденційності

Дотримання права на недоторканність приватного життя і переваг конфіденційності є невід'ємною частиною вирішення проблеми довіри до Інтернету. Ці права і очікування іноді зводяться до проблеми етичної обробки даних, підкреслюючи важливість задоволення очікувань дотримання прав конфіденційності і сумлінного використання даних. Інтернет речей здатний поставити під сумнів ці традиційні очікування дотримання прав приватного життя.

Проблеми конфіденційності, що виникли з появою Інтернету речей, дуже важливо вирішити, так як вони стосуються основних прав людини і здатності нашого суспільства довіряти Інтернету і підключеним до нього пристроям.

Інтернет речей часто представляється масштабної мережею сенсорних пристроїв, які збирають дані про оточення і нередкоо людей. Звичайно, ці дані можуть бути корисними для власників пристроїв, але дуже часто вони представляють інтерес і для виробників і постачальників пристроїв. Збір і використання даних перетворюється на справжню проблему конфіденційності, коли уявлення людей, що знаходяться під наглядом IoT-пристроїв, про масштаб і використанні даних, відрізняються від міркувань збирача даних.

Здаються нешкідливими комбінації потоків IoT-даних також можуть загрожувати конфіденційності. При об'єднанні або зіставленні кількох потоків даних іноді можна отримати більш точний цифровий портрет людини, ніж при використанні одного потоку IoT-даних. Наприклад, підключена до Інтернету зубна щітка може записувати і передавати нешкідливі дані про те, як її власник чистить зуби. Але якщо його холодильник передає дані про те, що він їсть, а фітнес-трекер передає дані про його фізичної активності, то комбінація цих потоків дозволяє отримати більш детальне і точне опис загального стану здоров'я цієї людини. Цей ефект групування даних може бути особливо справедливим по відношенню до IoT-пристроїв, так як багато пристроїв генерують додаткові метадані, наприклад, час і місце розташування, які дозволяють отримати більш конкретну інформацію про людину.

В інших ситуаціях користувач може не знати, що IoT-пристрій збирає дані про нього і здатне передавати їх третім сторонам. Цей тип збору даних отримує все більш

широке поширення в області побутових пристроїв, таких як розумні телевізори і ігрові приставки. Такі пристрої оснащені функцією розпізнавання голосу і зображення і тому можуть безперервно слухати або переглядати те, що відбувається в приміщенні і активно передавати ці дані в хмарний сервіс для подальшої обробки, і в цьому процесі іноді задіяні треті сторони. Людина може перебувати в оточенні подібних пристроїв, не підозрюючи про те, що його розмови або дії відстежуються, а дані записуються. Такого роду функції можуть не тільки приносити користь обізнаним користувачам, але і створювати проблеми конфіденційності тим, хто не підозрює про присутність цих пристроїв і не може контролювати використання зібраних даних.

Незалежно від того, чи відомо це користувачеві і чи згоден він з тим, що його дані збираються і аналізуються, подібні ситуації лише підкреслюють цінність персоналізованих потоків даних для компаній і організацій, які прагнуть збирати і записувати IoT-дані. Потреба в цих даних призводить до появи юридичних і нормативних проблем, пов'язаних з законами про захист і конфіденційність даних.

Ці проблеми конфіденційності важливо вирішити, так як вони впливають на основні права людини і його здатність довіряти Інтернету. В цілому люди усвідомлюють, що їхнє приватне життя дійсно представляє цінність, і у них є очікування у тому, що стосується збору та використання даних третіми сторонами. Це загальне уявлення про недоторканність приватного життя стосується і даних, що збираються IoT-пристроями, але ці пристрої можуть загрожувати можливості користувача висловлювати і домагатися дотримання його прав на приватне життя. Якщо користувач втратить довіру до Інтернету через недотримання його прав на приватне життя в Інтернеті речей, загальна цінність Інтернету може зменшитися.

1.5.3 Проблема інтероперабельності і стандартів

У традиційному Інтернеті интероперабельность пристроїв являє собою ключову цінність. Найважливіша вимога кІнтернетподключенію полягає в тому, щоб пов'язані системи були здатні говорити на одній мові протоколів і кодів. Інтероперабельність настільки важлива, що перші майстерні та семінари для постачальників Інтернет-обладнання так і називалися: Interops (від англ. Interoperability - інтероперабельність). Крім того, вона є ключовим моментом, на який звернено увагу всієї спільноти розробки Інтернет-стандартів, сконцентрованого навколо цільової інженерної групи Інтернету (IETF).

Інтероперабельність також є наріжним каменем відкритого Інтернету. Бар'єри, навмисно споруджуються, щоб перешкодити обміну інформацією, можуть позбавити користувачів Інтернету можливості підключатися, говорити, обмінюватися інформацією і пропонувати інновації, порушуючи чотири фундаментальних принципи ISOC. Так звані закриті платформи, де користувачі мають можливість взаємодіяти лише в рамках обмеженого набору веб-сайтів і сервісів, можуть значно знизити соціальні, політичні та економічні переваги від доступу до необмеженого Інтернет-простору.

В умовах повної інтероперабельності будь IoT-пристрій могло б встановлювати зв'язок з будь-яким іншим пристроєм або системою і виробляти бажаний обмін інформацією. Але на практиці интероперабельность є більш складним явищем. Взаємодія між IoT-пристроями і системами відбувається на різних рівнях і в різних шарах в рамках стека комунікаційних протоколів між пристроями. Крім того, полнаяінтероперабельность по всьому діапазону технічної продукції не завжди здійсненна, необхідна або бажана, особливо якщо нав'язувати її штучно (наприклад, на вимогу влади), що може послужити бар'єром для інвестицій і інновацій.

Стандартизація та прийняття протоколів, що визначають принципи зв'язку (в тому числі реальну потребу в наявності стандартів), є основною темою дискусій, що стосуються Інтернету речей.

Крім технічних аспектів, интероперабельность значно впливає на потенційне економічне вплив Інтернету речей. Добре налагоджена і явно виражена інтероперабельность IoT-пристроїв здатна стимулювати інновації та ефективність виробників, збільшуючи тим самим глобальний економічний продукт. Більш того, реалізація існуючих стандартів, а при необхідності створення нових відкритих стандартів, дозволяє зменшити бар'єри для створення та впровадження нових бізнес-моделей, а також створює умови для масштабного зростання економіки.

Згідно зі звітом міжнародної консалтингової компанії, McKinsey Global Institute за 2015 рік, в середньому 40 відсотків валового продукту, який може бути створений індустрією Інтернету речей, реалізується лише завдяки інтероперабельності. Далі в звіті говориться, що інтероперабельність є необхідною умовою для вивільнення потенційного валового продукту в розмірі 4 трильйонів доларів США в результаті використання Інтернету речей в 2025 р при загальній вартості валового продукту в розмірі 11,1 трильйонів доларів США у всіх дев'яти сферах, проаналізованих інститутом McKinsey.I хоча деякі компанії бачать конкурентні переваги і економічні вигоди в розробці власних систем, загальні економічні можливості на ринку закритих систем можуть бути весь ма обмежені.

Крім того, інтероперабельність за своєю природою є великою цінністю як для індивідуальних, так і для корпоративних споживачів цих пристроїв. Завдяки їй їм стає легше вибирати пристрої з кращим функціоналом за вигіднішою ціною і об'єднувати їх в системи для спільної роботи. Покупці можуть відчувати сумніви, набуваючи IoT-продукти або послуги за відсутності гнучкості інтеграції, наявності складнощів для власників цих пристроїв, занепокоєння через залежність від постачальника або через морального зносу при зміні стандартів.

1.6 Постановка мети і завдання дослідження

Сучасні технології, такі як Інтернет речей дозволяють створювати системи автоматизації будівель, які, перш за все, забезпечують комфорт і безпеку експлуатації, пристосовуючи роботу пристроїв і підсистем до вимог споживачів або тих, хто займається експлуатацією. Також вони реалізують контроль доступу з різними рівнями пріоритету, здійснюють моніторинг параметрів роботи обладнання, моніторинг і запис подій, взаємодіють з системами охоронної та пожежної сигналізації і т. д.

На великих об'єктах (комерційного та громадського призначення) ці завдання все частіше вирішуються за допомогою єдиної інтегральної системи управління будівлею, доступ до якої для уповноважених працівників забезпечується через Інтернет.

Технологія Інтернету речей дозволяє створювати єдині центри управління інженерними системами будівлі з автоматичною установкою оптимальних режимів. Реалізація такої концепції дозволить вирішити проблеми енергозбереження і відповідно економії коштів, спрямованих на експлуатацію будівлі.

Інтелектуальна будівля являє собою єдиний комплекс, де узгоджено функціонують до 50 різних систем управління: освітленням, електроживленням, вентиляцією, кондиціюванням, доступом, ліфтами, водопостачанням і т.д. Це можуть бути як прості системи моніторингу, так і повністю автоматизовані системи. Останні розпізнають різні ситуації і автоматично реагують на зміни параметрів зовнішнього середовища, ґрунтуючись на певних алгоритмах.

Таким чином, метою магістерської роботи є підвищення ефективності організаційно-технічного управління комплексною безпекою, системою контролю доступу, а також енергопостачанням ВНЗ шляхом розробки відповідного методичного та алгоритмічного забезпечення. Об'єктом дослідження є вищий навчальний заклад, а

предметом - оптимізація споживання ресурсів ВНЗ з використанням технології Інтернету речей.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– проаналізувати концепцію Інтернету речей та її можливості;

– проаналізувати структуру ВНЗ і виконати огляд літератури для пошуку ефективних варіантів оптимізації роботи ВНЗ;

– розробити варіанти автоматизації господарської діяльності ВНЗ;

– реалізувати web-додаток для дистанційного керування освітлювальними приладами.

2 УПРАВЛІННЯ ДІЯЛЬНІСТЮ ВИЩОГО НАВЧАЛЬНОГО ЗАКЛАДУ

Вищий навчальний заклад, як і будь-який інший навчальний заклад, є освітнім установою. Освітня установа – це установа, що здійснює освітній процес, тобто реалізує одну або кілька освітніх програм і забезпечує утримання і виховання учнів. Значення освіти для функціонування держави важко переоцінити. Зміст освіти є одним з чинників економічного і соціального прогресу суспільства.

Розглянемо, які типи ВНЗ можна виділити у всьому різноманітті існуючих в Україні освітніх установ. В залежності від кількості і різноманітності типів діяльності, зазвичай виділяють такі типи вищих навчальних закладів: університет, академія, інститут і коледж.

Університет – вищий навчальний заклад, діяльність якого спрямована на розвиток освіти, науки і культури шляхом проведення наукових досліджень і навчання на всіх рівнях вищої, післявузівської та додаткової освіти з широкого спектру напрямків. Університет є центром освіти, науки і культури, сприяє поширенню наукових знань і здійснює культурно-просвітницьку діяльність серед населення.

Академія – це навчальний заклад університетського рівня, що здійснює свою діяльність переважно в одній з областей науки, техніки або культури. Академія є провідним науковим і методичним центром у сфері своєї діяльності, в широких масштабах що здійснює підготовку фахівців вищої кваліфікації і перепідготовку фахівців певної галузі.

Інститут – самостійний ВНЗ або частина університету або академії, реалізує професійні освітні програми по ряду напрямів науки, техніки і культури і веде наукові дослідження.

Коледж – самостійний навчальний заклад або частина університету, академії чи інституту, що реалізує неповні і повні освітні програми вищої професійної освіти.

Важливими ознаками при здійсненні класифікації ВНЗ є чисельність учня контингенту (персоналу) та територіальна розгалуженість ВНЗ. За чисельністю контингенту виділяють ВНЗ:

- малої чисельності (менше 1000 чол.);
- середньої чисельності (1000-5000 чол.);
- великою чисельністю (понад 5000 чол.).

За територіальною роздрібненості:

– зосереджений ВНЗ (навчальні корпуси та інфраструктура зосереджені на невеликій території);

– розподілений ВНЗ без освіти кампусу (розміщення навчальних корпусів та інфраструктури характеризується значною просторовою розподіленністю);

– розподілений ВНЗ з утворенням кампусу (навчальні корпуси та інфраструктура ВНЗ розподілені на значній території, при цьому виділяється центральна сукупність корпусів - кампус, зосереджена на невеликій території).

Візуальне представлення класифікації ВНЗ за територіальної роздрібненості представлено на рисунку 2.1 (а – зосереджений ВНЗ, б – розподілений ВНЗ без освіти кампуса, в – розподілений ВУЗ освітою кампуса).

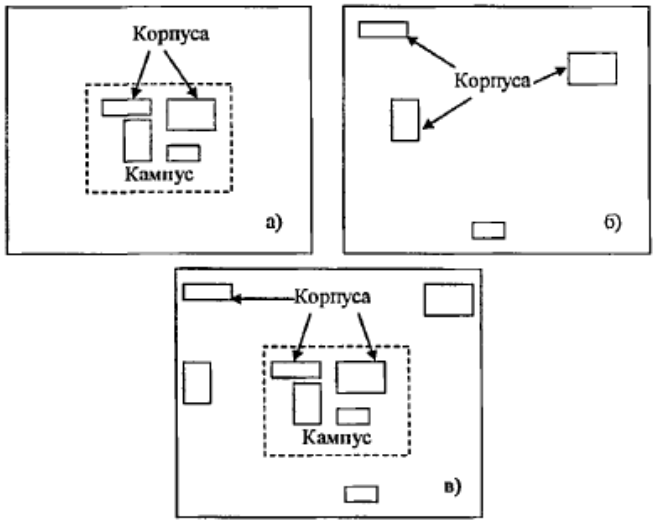


Рисунок 2.1 – Класифікація ВНЗ територіальної роздрібненості

Корінні зміни ролі знання в сучасному суспільстві, вимог з боку суспільства до вищим навчальним закладам, трансформація структури їх фінансування призвели до того, що університети почали активно розробляти стратегії своєї поведінки в зміненому і продовжує швидко змінюватися світі. Всі ці стратегії спрямовані на підвищення ефективності роботи університетів в нових умовах, адаптацію ВНЗ до ринкових відносин. Чимале значення для виконання даних завдань має створення ефективної системи управління ВНЗ, яка включає в себе оптимізацію освітлення і контролю доступу до ВНЗ. Ця система зможе внести свій відчутний внесок до забезпечення якості діяльності ВНЗ. Конкретний варіант застосовуваної системи оптимізації залежить від типу ВНЗ і є індивідуальним, однак, у принципі, є можливість виділити типові варіанти побудови системи оптимізації, які можуть застосовуватися для різних типів освітніх установ з невеликими змінами, які враховують особливості кожного ВНЗ.

2.1 Основні функції і структура сучасного ВНЗ

Як вже зазначалося, вищий навчальний заклад – це освітній заклад, що здійснює освітній процес, тобто реалізує одну або кілька освітніх програм і (або) забезпечує утримання і виховання учнів, вихованців.

Дерево функцій (основних видів діяльності) ВНЗ представлено на рисунку 2.2.

Рисунок 2.2 – Основні функції (види діяльності) НЗ

Виконання зазначених функцій здійснюється різними підрозділами ВНЗ. Структурна схема управління ВНЗ наведена на рисунку 2.3.

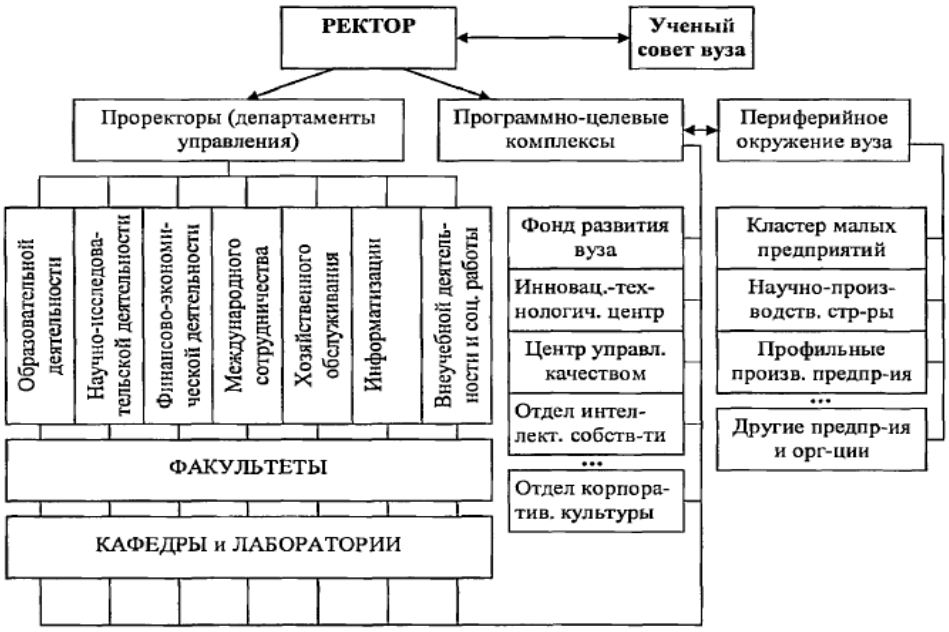


Рисунок 2.3 – Організаційна структура ВНЗ

Розкриємо внутрішній зміст головних функцій ВНЗ - освітньої і наукової. Для цього побудуємо семантичну мережу – узагальнену модель предметної області, що має вигляд графа, в якому вершини відповідають об'єктам предметної області, а дуги - відношенням між ними. Вказана семантична мережа представлена на рис. 2.4. Тут використовуються скорочення: ЛВС – локально-обчислювальна мережа, ПО – програмне забезпечення, АО – апаратне забезпечення.

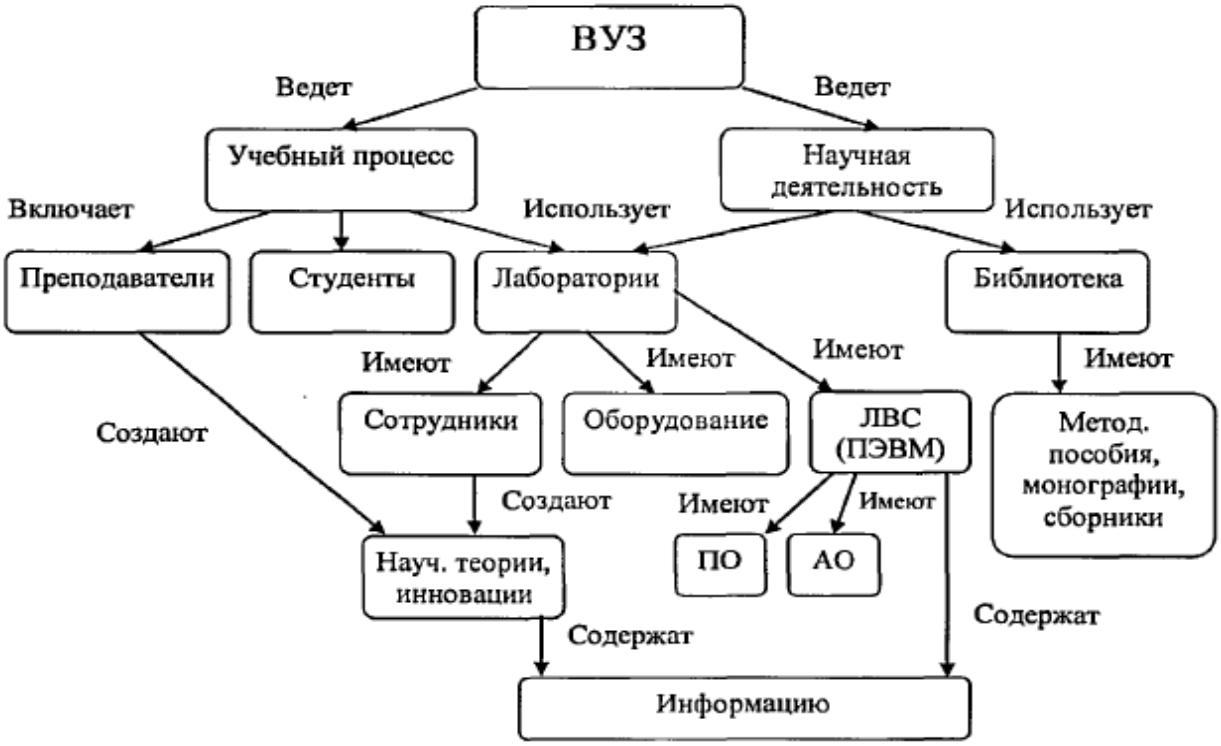


Рисунок 2.4 - Семантична мережа, що представляє діяльність ВНЗ

Проаналізувавши наведену мережу, а також взявши до уваги наявність інших функцій ВНЗ, можна зробити висновок, що для виконання своїх основних функцій ВНЗ використовує такі ресурси:

- матеріальні: приміщення, обладнання, ЛВС, ПЕОМ, книжкові фонди бібліотеки;

- людські: викладачі, студенти, співробітники;

- інформаційні: зміст і результати наукових досліджень відомості, що містять державну таємницю, фінансова документація, організаційно-розпорядча документація, особисті справи персоналу і студентів, інша інформація різного рівня важливості, що зберігається в електронному та паперовому вигляді.

Повна класифікація ресурсів ВНЗ наведено на рисунку 2.5.

Рисунок 2.5 - Класифікація ресурсів ВНЗ

2.2 Система управління безпекою ВНЗ

Різні засоби і системи контролю та управління доступом (СКУД), системи телевізійного спостереження (СТН) і безпеки, а також засоби інженерно-технічного енергоживлення вже давно застосовуються для забезпечення оптимізації та управління ВНЗ. Однак, на сьогоднішній день ці системи сильно застаріли і вони повинні бути замінені на нові, які зможуть забезпечити ті ж функції, але на більш високому рівні і при мінімальних витратах. Розвиток і впровадження нових технологій, матеріалів, комплектуючих та інших технічних і технологічних можливостей, створили нові умови для створення комплексних систем управління ВНЗ.

Системи комплексної безпеки або інтегровані системи безпеки, в останні роки знайшли широке застосування при організації охорони великих і особливої важливості об'єктів, таких як музеї, банки, сховища цінностей, адміністративні і житлові будівлі. Їх побудова відбувається шляхом об'єднання технічних засобів охоронної та охоронно-пожежної сигналізації (ОПС) з іншими технічними засобами охорони (ТСО) і безпеки в одну багатофункціональну систему з єдиним пунктом управління на об'єкті.

Новий етап у розвитку КСБ почався з інтеграції функціональних і технічних рішень щодо захисту об'єктів від несанкціонованого проникнення з технічними засобами охоронної та пожежної сигналізації, відеоспостереження, засобами протипожежної автоматики та іншими засобами захисту. Що ж це таке - комплексна система безпеки? Це одна з складових системи забезпечення комплексної безпеки (СОКБ). СОКБ - це сукупність методів і засобів підтримки безпечного стану об'єкта, запобігання, виявлення і

ліквідації загроз життю, здоров'ю, природному середовищу, майну та інформації. Під сукупністю методів і засобів маються на увазі як органи та виконавці служб охорони і безпеки і використовувані ними засоби і техніка, так і правові, організаційно-розпорядчі та нормативні документи в області забезпечення безпеки. За визначенням, СОКБ може включати в себе наступні компоненти (рис. 2.6):

- службу охорони і безпеки;
- адміністративний і операторський складу управління системою;
- технічний персонал, що обслуговує систему;
- систему правової та нормативної документації;
- комплексну систему безпеки (або КТСБ).

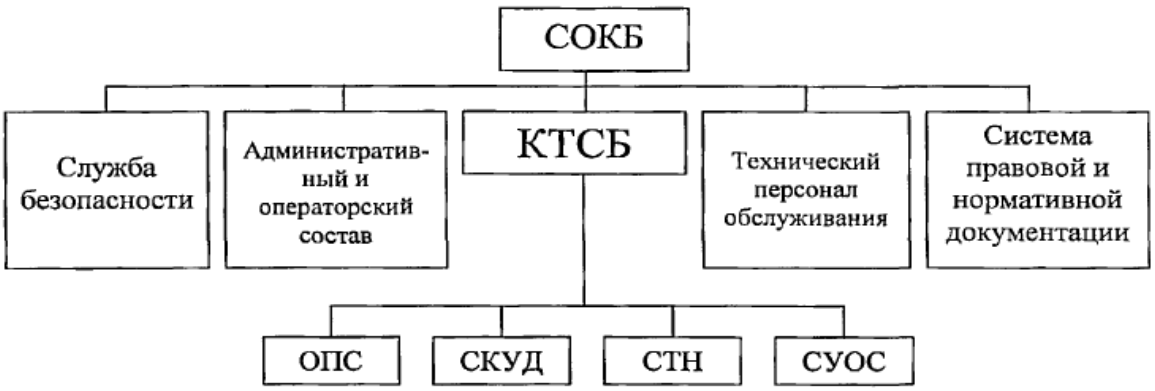


Рисунок 2.6 – Структура забезпечення комплексної безпеки ВНЗ

Під КТСБ при цьому розуміється сукупність усіх технічних засобів захисту і охорони, функціональних та інтегрованих, автономних і централізованих систем, що забезпечують безпеку і захист об'єкта за встановленим для нього показників і рівнів захищеності. Засоби і системи мають володіти технічної, програмної, інформаційної та експлуатаційної сумісності. Найбільш часто до складу КТСБ включають:

- систему охоронно-пожежної сигналізації (ОПС);
- систему контролю та управління доступом (СКУД);
- систему телевізійного спостереження (СТН);
- систему управління, оповіщення і зв'язку (СУОС).

Розглянемо перераховані компоненти КТСБ окремо.

Охоронно-пожежна сигналізація (ОПВ) – це комплекс технічних засобів, службовців для своєчасного виявлення несанкціонованого проникнення в охоронювану зону або виникнення пожежі. До її складу входить:

- обладнання централізованого управління охоронно-пожежною сигналізацією;

– устаткування збору і обробки інформації з датчиків охоронно-пожежної сигналізації (приємно-контрольні прилади, охоронно-пожежні панелі);

– сенсорні пристрої (датчики і сирени охоронно-пожежної сигналізації).

Система охоронної сигналізації забезпечує своєчасне оповіщення служби охорони про факт несанкціонованого проникнення або спробі проникнення людей в будівлю або його окремі приміщення з фіксацією дати, місця і часу порушення рубежу охорони. Система пожежної сигналізації забезпечує своєчасне виявлення місця загоряння, формування керуючих сигналів для систем оповіщення про пожежу та автоматичне пожежогасіння.

Інтеграція охоронної та пожежної сигналізації у складі єдиної системи ОПС здійснюється на рівні централізованого моніторингу та керування. Система контролю і управління доступом (СКУД) - забезпечує контроль доступу осіб на територію об'єкта, дозволяє вести суворий облік відвідувань, організовувати розмежування прав доступу і часу доступу на об'єкти. Дозвіл і реєстрація проходу через двері, хвіртки і турнікети засновані на ідентифікації носіїв інформації (карти, брелка, відбитка пальця і т. д.) зчитувальними пристроями. Вхід до приміщення можливий лише з використанням носіїв інформації (кодів) індивідуального користування. Всі факти пред'явлення носіїв інформації і пов'язані з ними дії фіксуються в контролері і зберігаються в комп'ютері.

Система телевізійного спостереження (СТН). У СТН використовується базове властивість будь-якої телевізійної системи - ефект присутності або дальнобачення. Можливість спостерігати з різних точок як розвиваються події, є основою для прийняття зважених, адекватних обстановці, оптимальних у даній ситуації рішень. Це приводить в остаточному підсумку до економічної вигоди, як від скорочення чисельності охоронців, так і від підвищення ефективності їх роботи завдяки своєчасному та адекватному реагуванню на події.

На сучасному етапі розвитку систем безпеки відбувається інтеграція системи охоронного телебачення з системами контролю і управління доступом, а також охоронної та пожежної сигналізації [13]. При отриманні тривожного сигналу від датчиків ОПВ, СТН автоматично виведе зображення відповідних телекамер на монітори оператора поста охорони і почне відеозапис. Процес об'єднання систем безпеки може йти двома шляхами:

– програмно-апаратна інтеграція;

– програмна інтеграція.

Програмно-апаратна інтеграція використовується виробниками систем безпеки. Загальна системна шина об'єднує апаратні пристрої систем охоронної, пожежної,

тривожної сигналізації, відеоспостереження та СКУД. Програмне забезпечення дозволяє конфігурувати, управляти і відображати стан будь-якого пристрою в системі. Програмна інтеграція використовується для об'єднання обладнання систем безпеки, зазвичай різних виробників, загальною води управління.

В даний час на ринку інтегрованих систем безпеки пропонуються різні програмно-апаратні рішення, розроблені як вітчизняними фірмами (НВП «Болід», ISS, «Сигма-ІС» та ін), так і зарубіжними компаніями (Simplex Grinnell, Lenel Systems International та ін).

Перевага інтегрованих систем безпеки над окремими системами неоднозначно. Взагалі кажучи, безпека об'єктів може бути ефективно забезпечена і роботою комплексу роздільних систем безпеки, а не єдиною інтегрованою системою безпеки, в силу наявності у останнього ряду серйозних недоліків. Інтегровані системи безпеки в даний час мають наступні недоліки:

- недостатню надійність;
- недостатню гнучкість в адаптації до умов роботи на конкретному об'єкті;
- надмірну інформативність;
- незручність інтерфейсів.

В інтегрованих системах безпеки функції управління, відображення і сигналізації передаються комп'ютеру. При його виході з ладу інтегрована система безпеки перестає функціонувати в повному обсязі. Таким чином, для надійного функціонування інтегрованої системи безпеки потрібна така її побудова, щоб при відключенні комп'ютера його функції переходили до самостійних апаратних пристроїв керування, тобто щоб система розпадалася на окремі, нормально функціонуючі системи.

Підкреслимо, що сьогодні потрібні в першу чергу такі системи, при спільній роботі яких досягається максимальний рівень безпеки об'єкта. Відбір обладнання конкретного виробника повинен проводитися не під впливом моди або престижністю, а виходячи з вимог найбільшої надійності і функціональності.

На сьогоднішній день величезне значення набуває завдання забезпечення безпеки, контролю доступу та оптимізація освітлення вищих навчальних закладів, у стінах яких працює та навчається велика кількість висококваліфікованих педагогічних працівників, наукових співробітників та молоді, складовою інтелектуальний і трудовий потенціал нашої країни. Підвищена небезпека пожеж, доступ сторонніх осіб, вчинення крадіжка також загострює проблему забезпечення безпеки матеріальних, фінансових, а також людських ресурсів ВНЗ.

Метою даної дипломної роботи є підвищення ефективності організаційно-технічного управління комплексною безпекою, системою контролю доступу, а також енергопостачанням ВНЗ шляхом розробки відповідного методичного та алгоритмічного забезпечення. В якості основної технології буде використовуватися технологія Інтернету речей, яка має величезний потенціал розвитку і дешеву елементну базу.

3 АВТОМАТИЗАЦІЯ ОСВІТЛЕННЯ І СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

Для досягнення поставленої мети була запропонована структура системи керування освітленням ВНЗ, яка базується на використанні датчиків руху і освітлення, що дозволило б проводити аналіз освітленості приміщення (аудиторії, кабінети, коридори) і підлаштовувати інтенсивність освітлення в залежності від умов і часу доби. Це дозволить знизити споживання електроенергії та внаслідок чого знизиться витрати на оплату електроенергії.

Другий не мало важливий фактор, це забезпечення контролю доступу. Система контролю доступу є майже обов'язковим елементом багатьох комплексних систем безпеки. І абсолютно виправдано, адже система контролю і управління доступом дозволяє автоматично контролювати не тільки вхід людей в будівлю або приміщення, але і вихід з нього, будучи ефективним засобом захисту від проникнення сторонніх осіб на територію об'єкта. Внаслідок цього контроль доступу допомагає забезпечити не тільки збереження матеріальних цінностей, але і безпеку персоналу організації. Крім запобігання доступу сторонніх, установка систем контролю доступу дозволяє розмежувати прохід співробітників і відвідувачів у відповідальні приміщення організації. Крім системи контролю доступу, також приділимо увагу системі безпеки і відеоспостереження. Камери з функцією виявлення руху будуть записувати дані і передавати їх по мережі тільки якщо в зоні їх огляду що-небудь відбувається. Це дозволяє значно зменшити обсяг пристроїв зберігання даних. У разі виникнення інциденту ви можете зрозуміти, коли і що саме сталося і хто винуватець інциденту, після чого зробити необхідні дії. Завдяки функціям автоматичного повідомлення ви зможете негайно отримати повідомлення про те, що трапилося і максимально оперативно прийняти необхідні заходи.

3.1 Автоматизація і керування освітленням

Актуальність проблеми енергозбереження у ВНЗ пов'язана з тим, що освітні установи є найбільшими споживачами енергоресурсів серед усіх державних установ України. При цьому споживання енергоресурсів у них на 1 метр квадратний площі в 2-4 рази вище, ніж у країнах Західної Європи, США і Канади. Крім того, питомі витрати на комунальні послуги в освітніх установах щорічно збільшуються на 25-30%. Аналіз

показав, що в українських університетах щороку зростає енергоспоживання, також, як і тарифи на енергоресурси, і загальні комунальні платежі.

Енергозбереження досягається завдяки використанню якісного світлотехнічного обладнання в поєднанні з датчиками руху, освітленості, а також налаштування системи у відповідності з заданими параметрами, наприклад, за часом. Освітлення може автоматично вмикатися і вимикатися у відповідності з режимом робочого часу і присутністю людей у приміщенні, а протягом дня необхідний рівень освітленості підтримується з урахуванням наявності в приміщенні природного світла. Поряд з енергозбереженням, використання системи управління освітленням дозволяє вирішити цілий ряд інших завдань на об'єкті, а саме:

– створити комфортні умови роботи для співробітників, навіть якщо в приміщенні відсутнє природне освітлення;

– забезпечити зручність керування режимами освітлення;

– значно знизити витрати на оплату електроенергії.

Домогтися найбільш повного і точного обліку наявності денного світла, так само як і обліку присутності людей в приміщенні, можна, застосовуючи засоби автоматичного управління освітленням (СУО). Управління освітлювальної навантаженням здійснюється при цьому двома основними способами: відключенням всіх або частини світильників (дискретне управління) і плавним зміною потужності світильників (однаковим для всіх або індивідуальним).

До систем дискретного управління освітленням в першу чергу належать різні фотореле (фотоавтомати) і таймери. Принцип дії перших заснований на включенні і відключенні навантаження за сигналами датчика зовнішньої природної освітленості. Другі здійснюють комутацію освітлювальної навантаження в залежності від часу доби за попередньо закладеною програмою. До систем дискретного керування освітленням відносяться також автомати, оснащені датчиками присутності. Вони відключають світильники в приміщенні через заданий проміжок часу після того, як з нього видаляється остання людина. Це найбільш економічний вид систем дискретного управління, проте до побічних ефектів їх використання належить можливе скорочення терміну служби ламп за рахунок частих включень і виключень.

Системи плавного регулювання потужності освітлення по своєму пристрою дещо складніше. Останнім часом багатьма зарубіжними фірмами освоєно виробництво обладнання для автоматизації керування внутрішнім освітленням. Сучасні системи

управління освітленням поєднують в собі значні можливості економії електроенергії з максимальною зручністю для користувачів.

3.1.1 Основні функції автоматизованих систем управління освітленням

Автоматизовані системи управління освітленням, призначені для використання в громадських будівлях, виконують наступні типові функції:

– точне підтримання штучної освітленості в приміщенні на заданому рівні. Досягається це введенням в систему управління освітленням фотоелемента, що знаходиться всередині приміщення і контролюючого створюється освітлювальною установкою освітленість;

– облік природної освітленості в приміщенні. Ця функція може здійснюватися тим же фотоелементом, що і в попередньому випадку, за умови, що він відстежує повну освітленість. При цьому економія енергії може становити 20 - 40%;

– облік часу доби і дня тижня. Для її реалізації автоматизована система управління освітленням повинна бути обладнана власними годинником реального часу;

– облік присутності людей в приміщенні. Одержувана за рахунок відключення світильників за сигналами таймера і датчиків присутності економія електроенергії становить 10 - 25%.

3.1.2 Приклад автоматизації системи управління освітленням

По запрограмованому в комп'ютері розкладом система управління, побудована на базі модуля реле, автоматично переводить на час занять люмінесцентне або світлодіодне освітлення коридорів, холів і зон рекреації в економічний режим, програмований в діапазоні 10-20% від номінальної потужності.

Якщо в системі не використовуються датчики руху, контролер підтримує встановлену мінімальну потужність системи освітлення коридорів до кінця поточного заняття, а після подачі дзвінка на переміну знову переводить освітлення в режим номінальної яскравості.

Якщо в системі управління використовуються датчики руху, які підключаються до модулю реле, то їх спрацьовування при проходженні людини по коридору під час уроків

призводить до автоматичного плавного збільшення світлового потоку групи світильників в контрольованій датчиком зоні. Потужність світильників регулюється плавно в діапазоні 2-100% від номінального значення. Передбачена зв'язок з системою пожежної сигналізації будівлі – при виникненні пожежі контролер переводить систему освітлення коридорів і холів в режим максимальної потужності для забезпечення нормальної евакуації людей з будівлі та гасіння пожежі. Можливий режим ручного управління освітленням, минаючи контролер і комп'ютер – звичайним вимикачем.

Рівень природного сонячного світла в звичайному будинку розподіляється нерівномірно - чим ближче до вікна розташовані парти, тим більш інтенсивно вони освітлені сонячним світлом і навпаки. Стандартне штучне освітлення не враховує цю особливість. Таким чином, коли природного світла недостатньо для віддаленого ряду парт, викладач зобов'язаний включити освітлення всієї аудиторії, в результаті чого більшу частину часу ближні до вікон ряди парт виявляються надмірно освітленими, що призводить до необґрунтованого витрачання електроенергії.

Підвищити ефективність систем освітлення аудиторії можна шляхом установки датчиків постійної освещенности К2110 на стелі над кожним рядом парт, як це зображено на рисунку 3.3.

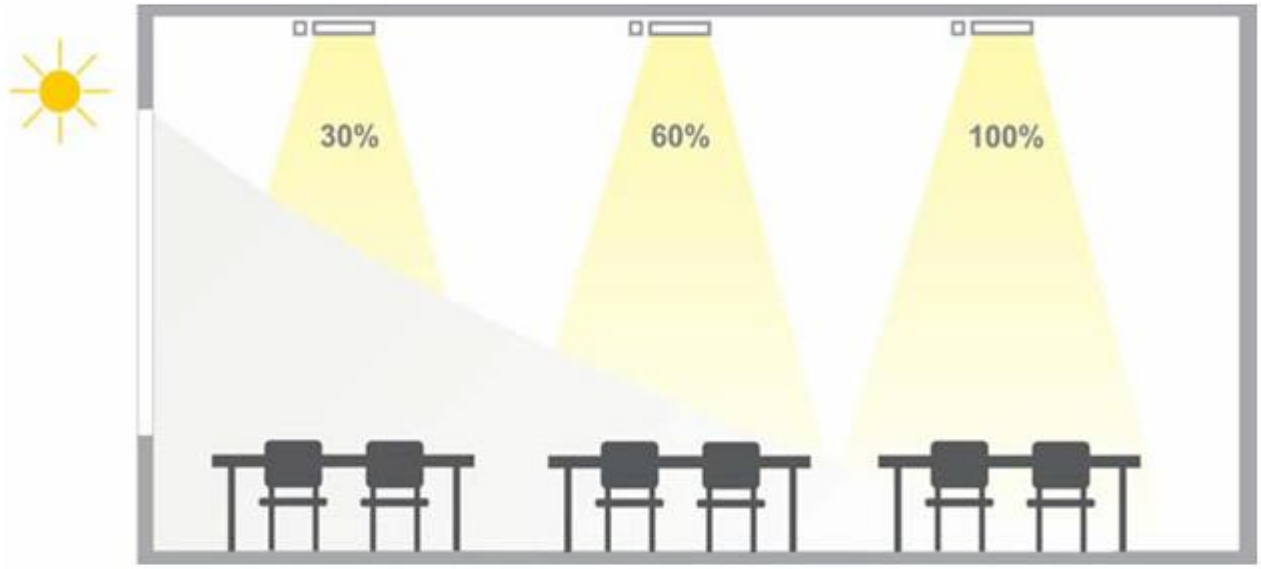


Рисунок 3.3 – Автоматичне управління освітленням аудиторії

Цей датчик здатний підтримувати заданий рівень освітленості, автоматично зменшуючи або збільшуючи світловий потік групи світильників в залежності від рівня

сонячного світла, проникаючого в аудиторію через вікна. У світлий час доби світильники, розташовані ближче до вікон (рис. 3.4) будуть працювати з меншою потужністю.

Рисунок 3.4 – Розташування датчиків освітлення в аудиторії

Рисунок 3.5 – Наочне зображення роботи датчика освітлення

На представленому рис. 3.5 наочно видно, як в сонячний день працюють датчики К2110: світильники, розташовані біля вікон, працюють у режимі мінімальної потужності (5% від номінального значення). Другий і третій ряди світильників також працюють в економічних режимах (приблизно 20% і 60% від номінальної потужності відповідно).

3.2 Система контролю доступом

На сьогоднішній день система контролю і управління доступом є невід'ємним елементом інфраструктури сучасного офісу подібно системі кондиціонування або системи електронного документообігу. Крім того, система контролю доступу є майже обов'язковим елементом багатьох комплексних систем безпеки. І абсолютно виправдано, адже система контролю і управління доступом дозволяє автоматично контролювати не тільки вхід людей в будівлю або приміщення, але і вихід з нього, будучи ефективним засобом захисту від проникнення сторонніх осіб на територію об'єкта. Внаслідок цього контроль доступу допомагає забезпечити не тільки збереження матеріальних цінностей, але і безпеку персоналу організації. Крім запобігання доступу сторонніх на територію ВНЗ, установка систем контролю доступу дозволяє розмежувати прохід співробітників і відвідувачів у відповідальні приміщення організації. Також установка системи контролю доступу на прохідні ВНЗ дозволяє автоматизувати роботу пункту охорони в бюро перепусток, виключаючи вплив людського фактора. Тим самим контроль управління доступом дозволяє впорядкувати прохід відвідувачів в приймальні організації.

Як вже було відмічено вище, найчастіше система контролю доступу для більшої ефективності інтегрується з іншими системами безпеки, наприклад, з системою відеоспостереження або охоронної сигналізацією. Крім того, просунуті системи контролю і управління доступом несуть в собі функціонал системи обліку робочого часу, що дозволяє вести контроль догляду та прибуття працівників на робоче місце. Таким чином, за допомогою системи контролю доступу, крім підвищення рівня безпеки організації відбувається ще і поліпшення дисципліни співробітників.

Сучасна система освіти зазнала значних змін. Раніше оцінки студентів складалися виключно з їх знань і вмінь. Зараз підсумкова оцінка студента складається з оцінки накопиченої в процесі навчання і оцінки за сам залік. Накопичена оцінка складається з успішності студента та його відвідуваності. От про саму відвідуваності студентів, а точніше про відстеження відвідуваності, і піде мова.

Прогули, запізнення, відсутність учнів на заняттях – це проблема кожного навчального закладу. Подібні помилки роблять процес навчання непередбачуваним, що в подальшому позначається на загальних показниках.

В даний час прийняті такі абревіатури: СКД - це система контролю доступу і СКУД - це система контролю і управління доступом. Відмінність СКУД від СКД саме в можливості подальшого перепрограмування системи безпеки щодо конкретних параметрів доступу. Так, наприклад, контролер СКУД на відміну від СКД дозволяє додавати і виключати дані щодо доступу для конкретних співробітників зі своєї системи з плином часу. Тобто СКУД вдає із себе більш гнучку систему безпеки в порівнянні з СКД.

3.2.1 Основні елементи системи контролю доступу

Сьогодні на українському ринку можна знайте продукцію СКУД від самих різних виробників. Альо основні елементи такої системи безпеки незмінні: це контролер управління, зчитувачі персональних ідентифікаторів, персональні ідентифікатори (біометрична система, смарт карти, різні жетони або брелоки з бездротовими мітками), а також пристрої узгодження і блокуючі пристрої.

Персональні ідентифікатори (кодоносители) видаються персоналу організації і використовуються в подальшому в якості пропусків на території офісу чи підприємства. Кожен такий ідентифікатор містить в собі унікальний код, який витягується зчитувачем при контакті з кодоносителем. Після чого персональний код ідентифікатора проходить аналіз по базі даних контролера СКД. У разі якщо код картки (брелока, touch memory і т. д.) відповідає визначеним критеріям допуску, автоматика подає сигнал на блокувальний пристрій і проводиться відкриття дверей, підйом шлагбаума і т. п. Персональні ідентифікатори розрізняються за протоколами зв'язку зі зчитувачами, тому при проектуванні СКУД необхідно, щоб зчитувач і ідентифікатор підтримували один і той же протокол зв'язку.

Зчитувачі СКУД, як вже було відмічено вище, відповідають за вилучення інформації з кодоносителя та її подальшу передачу контролеру системи. Мабуть, вибір зчитувача крім чисто технічних характеристик визначається ще й вимогами, які накладає інтер'єр приміщення, де встановлюється сам зчитувач.

Контролери СКД – найбільш важливий елемент у контролі доступу. Надійність і продуктивність контролерів СКУД сильно позначається на подальшій роботі всієї системи. Коли стоїть завдання вибору контролера без його подальшої зв'язку з керуючим

комп'ютером, слід приділити якнайпильнішу увагу наступним характеристикам: максимальне число користувачів (ідентифікаторів), наявність внутрішніх годин, кількість реєстрованих подій, підтримка програмованих правил і т. п.

Блокувальні пристрої - це шлагбауми, турнікети, електромеханічні і електромагнітні замки, хвіртки і шлюзи. Вибір блокуючого пристрою виконується виходячи з вимог конкретного об'єкта.

3.2.2 Організації системи контролю доступу

Існують різні конфігурації систем контролю управління доступом: найпростіші з них розраховані всього на одну вхідні двері, а самі складні призначені для контролю доступу на великих об'єктах підприємствах, заводах і банках. При цьому найпростіший варіант СКУД представляє з себе звичайний домофон. Незалежно від конфігурації СКУД, кожна подібна система складається з декількох обов'язкових вузлів, це контролери для управління, зчитувачі для ідентифікації, а також всілякі виконавчі пристрої обмеження доступу: турнікети, електромагнітні замки і заскочки. Електронні безконтактні картки в якості перепусток є самим поширеним і зручним засобом ідентифікації в системах контролю доступу.

Працює система контролю і управління доступом наступним чином: на прохідній підприємства, при вході у відповідальні приміщення встановлюються засоби контролю доступу: електромеханічні турнікети, електромеханічні або електромагнітні замки, зчитувачі безконтактних карт.

Всі ці пристрої підключаються до контролерів системи управління доступом. Контролери призначені для прийому і аналізу інформації про пред'являються картах доступу, а також для управління різними виконавчими пристроями. До складу обладнання системи контролю доступу можуть входити 2 типу контролерів: контролери замку і контролери турнікета, кожен з яких відповідає за контроль роботи власного сайту. Кожному співробітникові підприємства видається персональний ідентифікатор, найчастіше це виявляється безконтактна карта доступу – пластикова картка з унікальним електронним кодом. Але можливо і застосування магнітних карт або т. зв. Touch memory пристроїв. Цей ідентифікатор одночасно є перепусткою на прохідній організації та ключем від тих приміщень, куди співробітникові дозволений доступ.

Для проходу через турнікет або входу в відповідальна приміщення працівники підприємства повинні піднести свою карту доступу до зчитувача, після чого зчитувач

передає код пред'явленої картки в контролер, а контролер доступу приймає рішення про дозвіл або заборону проходу на підставі закладеної в нього інформації. У разі якщо доступ дозволений, система контролю доступу автоматично розблокує турнікет або замок на двері. Приклад такої організації мережі контролю доступу зображено на рисунку 3.6. Так, наприклад, контролер СКУД може бути запрограмований на пропуск конкретних співробітників в певні приміщення тільки в задані проміжки часу, скажімо, з 9 до 18 години. До контролера СКУД також можна підключити охоронну сигналізацію, до складу якої входять охоронні датчики.

Також з допомогою СКУД можна здійснювати контроль в'їзду автотранспорту на територію об'єкта, в цьому випадку після пред'явлення персонального ідентифікатора відбувається відкриття воріт або підйом шлагбаума.

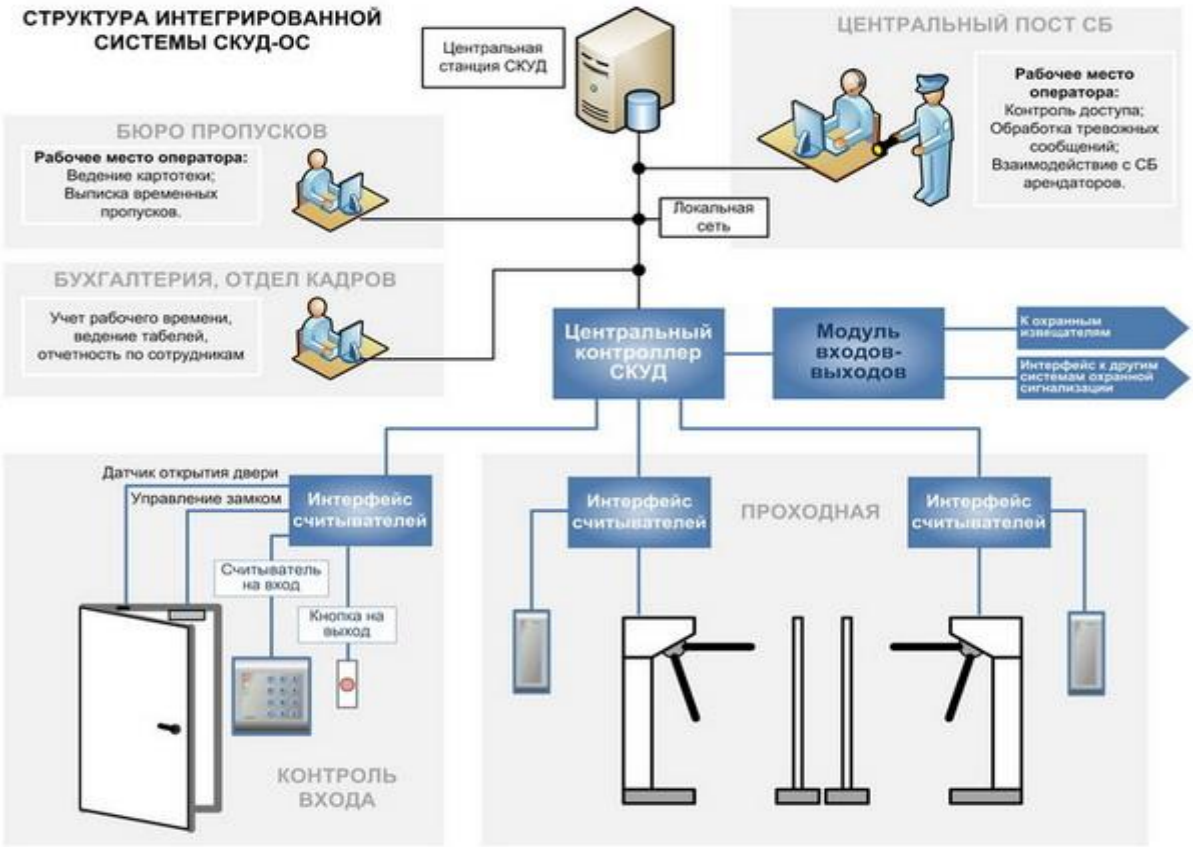


Рисунок 3.6 – Приклад організації мережі контролю доступу

3.2.3 Контроль відвідуваності

Однією з основних завдань завданням усіх навчальних СКУД є відстеження відвідуваності студентів і учнів безпосередньо на вході в будівлю. Дані системи

спрямовані на захист закладу від доступу до неї сторонніх. Далі описані принципи дії знайдених систем.

При вході в аудиторію де проходить лекція студенту необхідно піднести свій електронний пропуск до рідера. Рідер передає в контролер номер картки, який, у свою чергу, передає номер картки студента, використовуючи інтерфейс RS485.

Отримавши номер карти програмне забезпечення робить запит у базу даних і знаходить у ній інформацію про власника карти. Далі, отримавши інформацію про студента, виводить на екран інформацію та фото студента, і заносить в базу інформацію про час входу конкретного студента, що означає, що він відвідав лекцію. Принцип роботи системи показаний на рисунку 3.7.

Надалі звіти про свою відвідуваності можна буде побачити на спеціалізованому веб-сайті.

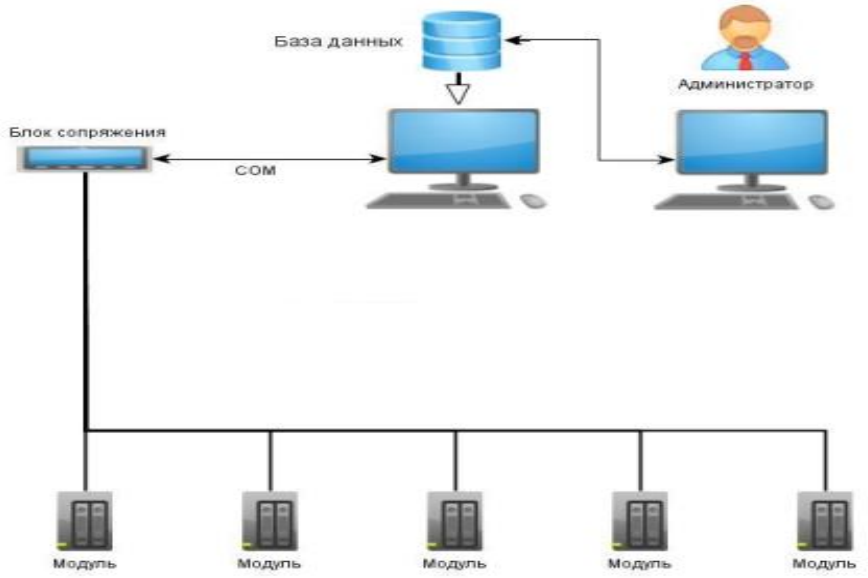


Рисунок 3.7 – Принцип роботи системи перевірки відвідування

Як можна помітити, контролери з'єднані одним зв'язком. Зроблено це для того, щоб мінімізувати кількість зв'язків з аудиторіями. Так само даний варіант з'єднання дозволяє нам використовувати один порт на сервері, що в свою чергу дозволяє нам полегшити написання і роботу на сервері.

Всі контролери передають номери карток студентів через загальну лінію. Програма повинна буде отримати кожен номер картки та ідентифікувати кожного користувача. В силу особливостей контролера (теоретично) зможемо отримувати інформацію про те, який конкретно контролер передав нам номер, визначаючи тим самим в яку аудиторію отримав доступ, входить студент.

Програмне забезпечення на сервері повинен буде отримувати номера карти з мінімальними затримками, тобто при великій кількості вхідних даних всі вони повинні бути оброблені. Це можна забезпечити кількома способами:

– записувати номери карт в тимчасовий файл і при припиненні прийому даних обробляти отримані дані;

– записувати номери карт в масив даних і в окремому потоці обробляти їх на льоту;

– обробляти одержані дані безпосередньо при отриманні.

Із запропонованих варіантів задовольняє нашим вимогам варіант номер два, так як у міру отримання даних вони будуть відразу ж оброблятися, але в окремому потоці. Даний варіант передбачає відсутність навантаження на процес отримання даних, так як процес отримання даних та їх обробки виконуються в різних потоках, незалежних один від одного.

Після отримання даних програмне забезпечення створює в базі даних запис про ввійшов студента або співробітника в аудиторію. В базі буде міститися: номер картки вхідного, прізвище, ім'я та по батькові, час входу і час виходу з аудиторії. У разі, якщо студент або співробітник забуде відзначитися при виході з аудиторії – система автоматично виведе людину з аудиторії при наступному заході в будь-яку іншу аудиторію.

У процесі розробки системи планується розробити web-інтерфейс для відстеження відвідуваності батьками і самими студентами.

Даний інтерфейс буде спрямований і на викладачів. Після початку заняття викладач зможе відкрити особисту сторінку і побачити присутніх і відсутніх студентів, перевірити їх присутність повторно, у разі сумнівів і скоригувати дані в системі.

Щодо роботи системи в плані організації навчального процесу навчальною частиною: у навчальній частині буде відповідне програмне забезпечення, для оповіщення співробітників про відсутніх студентів. Особливо важливо відслідковувати відвідуваність студентів на заліках або іспитах.

Основним недоліком системи буде неточність контролю відвідування студентами лекцій. Основні причини:

– студент може передати карту іншому студенту;

– студент може відзначитися на вході, але не зайти в аудиторію.

Дані недоліки виправити практично неможливо.

Можливі варіанти вирішення проблеми:

- встановлення обладнання з великим радіусом зчитування карт;
- фото/відео фіксація відвідування студентом лекцій;
- ручна повторна перевірка викладачем.

4 ПРОГРАМНА ТА АПАРАТНА РЕАЛІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ

Інтернет речей є однією з основних технологій для створення системи контролю та управління розумним будинком, промисловими підприємствами, а також вищими навчальними закладами. Основна ідея полягає в підключенні різних приладів, датчиків, пристроїв, об'єднаних в мережу за допомогою будь-яких доступних каналів зв'язку, що використовують різні протоколи взаємодії між собою і єдиний протокол доступу до глобальної мережі.

Для організації такого роду системи знадобиться контролюючі пристрій, яке буде здійснювати збір і передачу даних з підключених у систему датчиків. В даній роботі в якості контролюючого пристрою був обраний мініатюрний комп'ютер Raspberry Pi 2 Model 2, який і буде здійснювати збір і пересилку даних. Вибір цього пристрою був зумовлений наявністю потужного 4-х ядерного процесора ARM, невеликі габарити, наявність роз'єму Ethernet, відносно невисока вартість і найголовніше: 40-а піновий GPIO порт, до якого підключаються пристрої і датчики.

Для демонстрації можливостей технології Інтернету речей, я реалізував web-додаток для дистанційного керування освітлювальними приладами і обігрівачем. Цей додаток має мінімальний функціонал і примітивний інтерфейс, проте воно здатне виконувати наступні функції:

– віддалене включення і виключення двох електро-розеток, перша розетка служити для підключення електронагрівача, а друга - стандартні лампи розжарювання;

– визначення температуру в приміщенні;

– розетка для обігрівача управлятися годиною, передбачено годину включення і виключення обігрівача, які вводитимуться в браузер.

Для реалізації інтерфейсу я використовував технології HTML, CSS3 і Python. Комбінація цих згаданих технологій є потужним інструментом для створення користувацьких інтерфейсів. Мова програмування Python дозволяє використовувати простий API для взаємодії з сервером. Каскадні таблиці стилів CSS корисні для стилізації різних елементів сторінки HTML. У разі коректного використання вони дозволяють створювати динамічні інтерфейси шляхом зміни стилів елементів сторінок при настанні тих чи інших подій. Для даного проекту я вибрав фреймворк Webiopi, який представляє пакет програм, спеціально розроблений для Raspberry Pi для віддаленого керування пристроями, Python для обробки подій, CSS для розміщення кнопок у формі

Webiopi дозволяє створювати різні користувальницькі додатки та на рисунку 4.1 показано основні можливість цього фреймворку.

Рисунок 4.1 - Можливості Webiopi

Таким чином Webiopi має наступні можливості:

– вбудований Web - сервер, реалізований на мові Python;

– вбудована підтримка більш ніж 30 пристроїв з інтерфейсами UART, SPI, I2C, 1-Wire;

– бібліотеки Javascript / HTML для створення Web-інтерфейсу;

– бібліотеки Python / Java для створення додатків під Android;

– бібліотеки підтримують протокол CoAP призначений для управління і взаємодії між простими електронними пристроями через мережу.

Webiopi має відкритий код, який може бути змінений користувачем. Це дозволяє збільшити кількість завдань для вирішення. Для установки пакета під конкретну задачу змінюється файл конфігурації. Наприклад, в цей файл записуються GPIO pins, до яких підключені пристрої. Якщо використовуються датчики, їх також заносять в конфігураційний файл.

Файл html з WebIOPi Javascript library повинен сформувати web сторінку, показану на рисунку 4.3, передавати на сервер команди при натисканні на кнопки, одержувати від сервера інформацію про стан кнопок, виводити значення дати, температури і взаємодіяти зі скриптом на Пітоні.

Завданням скрипта вище написане на Пітоні є отримання даних з температурного датчика та передача їх в файл index.html.

Оголошень файлів index.html і script.py можна подивитися у додатку А.

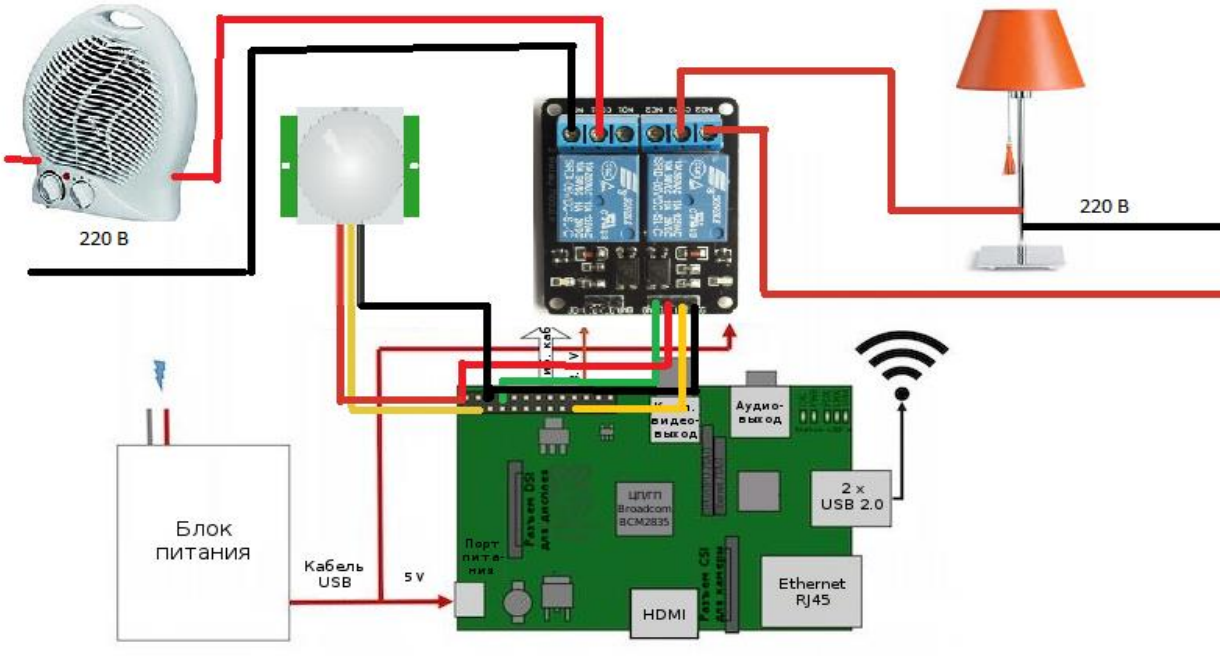


Рисунок 4.2 – Схема підключення апаратної частини

На рис. 4.2 представлена схема підключення релейного модуля до пинам порту GPIO Raspberry Pi і мережі 220 В. Наведене на малюнку підключення працездатно, якщо реле спрацьовують від напруги 5 вольт. Необхідно відзначити, що реле спрацьовує при подачі на вхід модуля нульової напруги. Скріншот додатка представлений на рисунку 4.3.

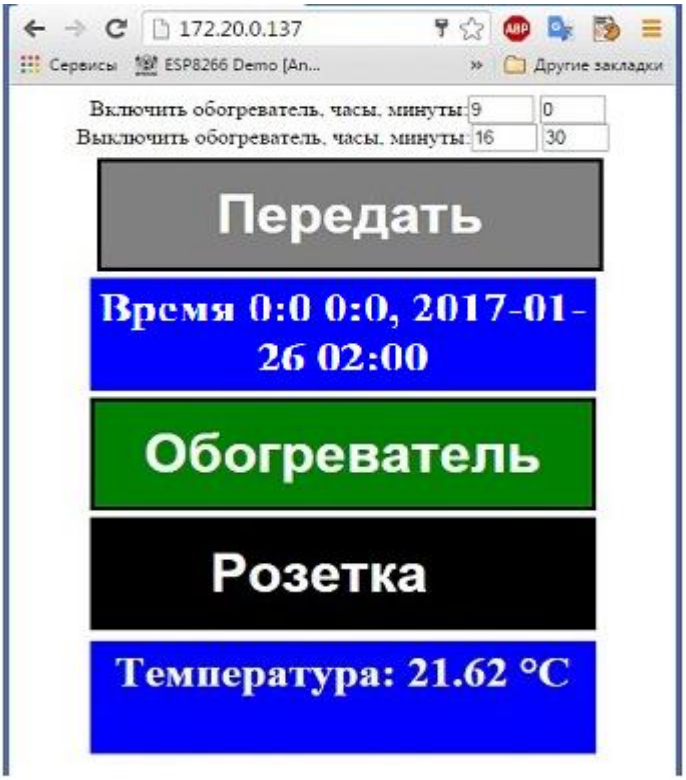


Рисунок 4.3 – Графічний інтерфейс програми

В ході написання атестаційної роботи був проведений невеликий експеримент, який полягав у вимірі споживаної потужності освітлювальних ламп. На протязі одного тижня з допомогою мобільного лічильника електроенергії Lemanso, який підключався у електричну ланцюг, проводилися виміри споживання електроенергії двома освітлювальними лампами в режимі звичайного використання.

Рисунок 4.4 Вимірювач потужності електроенергії приладів Lemanso LM669

Через тиждень, у систему освітлення ламп були додані датчики руху і присутності, які автоматично вимикали освітлення, якщо в радіусі їх дії не було виявлено руху протягом 5 хвилин. Це дозволило вимикати освітлення, якщо чоловік залишав кімнату на тривалий час, внаслідок чого марне використання електроенергії зводилося до мінімуму. Після двох тижнів вимірювань, на підставі отриманих результатів, був побудований графік показує різницю споживання електроенергії (рис. 4.5).

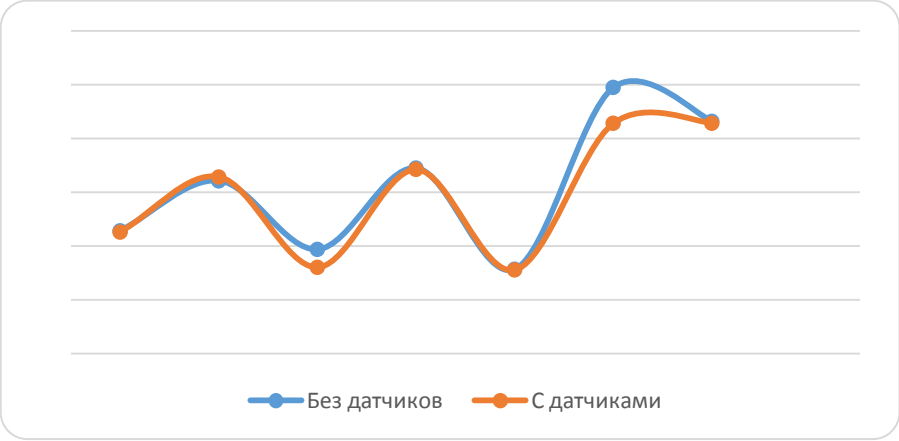


Рисунок 4.5 – Статистика споживання електроенергії по днях тижня.

5 ОХОРОНА ПРАЦІ ТА НЕБЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

5.1 Аналіз потенційних небезпечних і шкідливих виробничих чинників проектованого об’єкту, що мають вплив на персонал

У магістерській роботі об’єктом розробки є програмний додаток, котрий призначено для організації системи автоматизації освітлення і системи контролю доступу у навчальному закладі. Розроблене програмне забезпечення орієнтоване на роботу з персональним комп'ютером. Експлуатовані для вирішення внутрішньовиробничих завдань ПЕОМ типу IBM PC мають наступні характеристики:

споживана потужність	220 Вт;
робоча напруга	220 В;
напруга джерел живлення	+12 В; - 12 В; +5 В;
робоча частота	50 Гц.

Виходячи з приведених характеристик, вочевидь, що для людини існує небезпека поразки електричним струмом, унаслідок недбалого поводження з комп'ютером і порушення правил експлуатації, залишення частин ПЕОМ, що знаходяться під напругою, відкритими або знятих для ремонту вузлів.

Відповідно до [46] до легкої фізичної роботи відносяться всі види діяльності, виконувані сидячи і ті, що не потребують фізичної напруги. Робота користувача ПК відноситься до категорії 1а.

При роботі на ПЕОМ користувач піддається ряду потенційних небезпек. Унаслідок недотримання правив техніки безпеки при роботі з машиною(невиконання огляду відкритих частин ПЕОМ, що знаходяться під напругою або знятих для ремонту вузлів) для користувача існує небезпека поразки електричним струмом.

Джерелами підвищеної небезпеки можуть служити наступні елементи:

- розподільний щит;
- джерела живлення;
- блоки ПЕОМ і друку, що знаходяться в ремонті.

Ще одна проблема полягає у тому, що спектр випромінювання комп'ютерного монітора включає рентгенівську, ультрафіолетову і інфрачервону області, а також широкий діапазон хвиль інших частот. Небезпека рентгенівського проміння мала, оскільки цей вид випромінювання поглинається речовиною екрану. Проте велику увагу

слід приділяти біологічним ефектам низькочастотних електромагнітних полів(аж до порушення ДНК).

Відповідно до [47], при обслуговуванні ПЕОМ мають місце фізичні і психофізичні небезпечні, а також шкідливі виробничі чинники:

– підвищене значення напруги в електричному ланцюзі, замикання якої може відбутися через тіло людини;
– підвищений рівень статичної електрики;
– підвищений рівень електромагнітних випромінювань;
– підвищена або знижена температура повітря робочої зони;
– підвищений або знижений рух повітря;
– підвищена або знижена вологість повітря;
– відсутність або недостатність природного світла;
– підвищена пульсація світлового потоку;
– недостатня освітленість робочого місця;
– підвищений рівень шуму на робочому місці;
– розумове перенапруження;
– емоційні навантаження;
– монотонність праці.

5.2 Заходи щодо техніки безпеки

Основним небезпечним чинником при роботі з ЕОМ є небезпека поразки людини електричним струмом, яка посилюється тим, що органи чуття людини не можуть на відстані знайти наявності електричної напруги на устаткуванні.

Проходячи через тіло людини, електричний струм чинить на нього складну дію, що є сукупністю термічної(нагрів тканин і біологічних середовищ), електролітичної(розкладання крові і плазми) і біологічної(роздратування і збудження нервових волокон і інших органів тканин організму) дій.

Тяжкість поразки людини електричним струмом залежить від цілого ряду чинників:

– значення сили струму;
– електричного опору тіла людини і тривалості протікання через нього струму;
– роду і частоти струму;

– індивідуальних властивостей людини і навколишнього середовища.

Розроблений дипломний проект передбачає наступні технічні способи і засоби, що застерігають людину від ураження електричним струмом [48]:

– заземлення електроустановок;

– занулення;

– захисне відключення;

– електричне розділення ятерів;

– використовування малої напруги;

– ізоляція частин, що проводять струм;

– огорожа електроустановок.

Занулення зменшує напругу дотику і обмежує година, протягом якого людина, ткнувшись до корпусу, може потрапити під дію напруги.

Струм однофазного короткого замикання визначається по наближеній формулі:

$$I_K = \frac{\text{Uф}}{\text{Zп} + \frac{\text{Zт}}{3}} , \qquad (5.1)$$

де Uф - номінальна фазна напруга мережі, В;

Zп - повний опір петлі, створене фазними і нульовими дротами, Ом;

Zт - повний опір струму короткого замикання на корпус, Ом.

Згідно таблиці 4 [49]: Zт /3 = 0,1 Ом.

Для провідників і жил кабелю для розрахунку повного опору петлі використовуємо формулу(4.2.) :

$$Z\text{п} = \sqrt{\text{Rп}^2 + \text{Xп}^2} , \qquad (5.2)$$

де Rп = Rф + Ro - сумарний активний опір фазного Rф і нульового Ro дротів, Ом;

Xп - індуктивний опір паяння дротів, Ом.

Перетин 1 км мідного дроту S = 2.5 мм, тоді згідно таблицям 5 і 6 [9], має такий опір:

Xп = 0,11 Ом;

Rф = 7,55 Ом;

Ro = 7,55 Ом.

Отже, Rп = 7,55 + 7,55 = 15,1 Ом.

Тоді по формулі (4.2) знаходимо повний опір петлі :

$$Zп = \sqrt{15,1^2 + 0,11^2} \approx 15,1 \text{ (Ом)}.$$

Струм однофазного короткого замикання рівний:

$$Iк = \frac{220}{15,1 + 0,1} = 14,47 \text{ (А)}.$$

Дія плавкої вставки на ПЕОМ забезпечується, якщо виконується співвідношення:

$$Iк \geq k * Iн, \qquad (5.3)$$

де Iн - номінальний струм спрацьовування плавкої вставки, А;

k - коефіцієнт кратності нелінійного струму Iн, А.

Коефіцієнт кратності нелінійного струму Iн розраховується по формулі (4.4.) :

$$Iн = P / U, \qquad (4.4)$$

де P = 220 Вт - споживана потужність;

U = 220 В - робоча напруга;

k = 3 А - для плавких вставок.

Отже, Iн = 220 / 220 = 1 А.

Підставивши значення у вираз (4.3), одержимо:

$$14,47 > 3*1.$$

Таким чином, доведено, що апарат забезпечить спрацьовування(і захист) при підвищенні номінального струму.

5.3 Заходи, що забезпечують виробничу санітарію і гігієну праці

Вимоги до виробничих приміщень встановлюються [50], СНіП, відповідними ГОСТами і ОСТамі з урахуванням небезпечних і шкідливих чинників, що утворюються в процесі експлуатації електроустаткування.

Підвищення працездатності людини і збереження її здоров'я забезпечується стабільними метеорологічними умовами. Мікроклімат виробничих приміщень [51] визначається діючими на організм людини поєднаннями температури, вологості і швидкості руху повітря, а також температури навколишніх поверхонь. Значне коливання параметрів мікроклімату приводити до порушення систем кровообігу, нервової і потовидільної, що може викликати підвищення або пониження температури тіла, слабкість, запаморочення і навіть непритомність.

Відповідно до [52] встановлюють оптимальну і допустиму температуру, відносну вологість і швидкість руху повітря в робочій зоні . За відсутності надмірного тепла, вологи, шкідливих речовин в приміщенні досить природної вентиляції.

У приміщенні для виконання робіт операторського типу(категорія 1а), пов'язаних з нервово-емоційною напругою, проектом передбачається дотримання наступних нормованих величин параметрів мікроклімату (табл. 4.1).

Таблиця 5.1 - Санітарні норми мікроклімату робочої зони приміщень для робіт категорії 1а.

Пора року	Температура, С	Відносна вологість, %	Швидкість руху повітря, м/с
Холодна	22…24	40…60	0,1
Тепло	23…25	40…60	0,1

У приміщенні, де знаходиться ПЕОМ, повітрообмін реалізується за допомогою природної організованої вентиляції(з пристроєм вентиляційних каналів в перекриттях будівлі і вертикальних шахт) й установленого промислового кондиціонера фірми Mitsubishi, який дозволяє вирішити переважну більшість завдань по створінню та підтримці необхідних параметрів повітряного середовища. Цей метод забезпечує приток потрібної кількості свіжого повітря, визначеного в СНіП (30 $м^3$ в годину на одного працівника).

Шум на виробництві має шкідливу дію на організм людини. Стомлення операторів через шум збільшує число помилок при роботі, призводить до виникнення травм. Для

оператора ПЕОМ джерелом шуму є робота принтера. Щоб усунути це джерело шуму, використовують наступні методи. При покупці принтера слід вибирати найбільш шумозахисні матричні принтери або з великою швидкістю роботи(струменеві, лазерні). Рекомендується принтер поміщати в найбільш віддалене місце від персоналу, або застосувати звукоізоляцію та звукопоглинання(під принтер підкладають демпфуючі підкладки з пористих звукопоглинальних матеріалів з листів тонкої повсті, поролону, пеноплену).

При роботі на ПЕОМ, проектом передбачені наступні методи захисту від електромагнітного випромінювання : обмеження часом, відстанню, властивостями екрану.

Обмеження годині роботи на ПЕОМ складає 3,5-4,5 години. Захист відстанню передбачає розміщення монітора на відстані 0,4-0,5 м від оператора. Передбачений монітор 20" TFT, Samsung 2043BW відповідає вимогам стандарту [53].

Стандарт [13] пред’являє жорсткі вимоги в таких областях: ергономіка(фізична, візуальна і зручність користування), енергія, випромінювання(електричних і магнітних полів), навколишнє середовище і екологія, а також пожежна та електрична безпека, які відповідають всім вимогам [54].

Для зниження стомлюваності та підвищення продуктивності праці обслуговуючого персоналу в колірній композиції інтер'єру приміщень для ПЕОМ дипломним проектом пропонується використовувати спокійні колірні поєднання і покриття, що не дають відблисків.

У проекті передбачається використання сумісного освітлення. У світлий час доби приміщення освітлюватиметься через віконні отвори, в решту часу використовуватиметься штучне освітлення.

Як штучне освітлення необхідно використовувати штучне робоче загальне освітлення. Для загального освітлення необхідно використовувати люмінесцентні лампи. Вони володіють наступними перевагами: високою світловою віддачею, тривалим терміном служби, хоча мають і недоліки: високу пульсацію світлового потоку.

При експлуатації ПЕОМ виробляється зорова робота. Відповідно до [55] ця робота відноситься до розряду 5а. При цьому нормоване освітлення на робочому місці(Ен) при загальному освітленні рівна 200 лк.

Приміщення завдовжки 12 м, шириною 10 м, заввишки 4 м обладнується світильниками типу ЛП02П, оснащеними лампами типу ЛБ зі світловим потоком 3120 лм кожна.

Виконаємо розрахунок кількості світильників в робочому приміщенні завдовжки a=12 м, шириною b=10 м, заввишки з=4 м, використовуючи формулу (4.5) розрахунку штучного освітлення при горизонтальній робочій поверхні методом світлового потоку:

$$n = (E \cdot S \cdot Z \cdot k)/(F \cdot U \cdot M), \quad (5.5)$$

де F - світловий потік = 3120 лм;

E - максимально допустима освітленість робочих поверхонь = 200 лк;

S - площа підлоги = 120 м2;

Z - поправочний коефіцієнт світильника = 1,2;

k - коефіцієнт запасу, що враховує зниження освітленості в процесі експлуатації світильників = 1,5;

n - кількість світильників;

U - коефіцієнт використовування освітлювальної установки = 0,6;

M - кількість ламп у світильнику =2.

З формули (4.5) виразимо n (4.6) і визначимо кількість світильників для даного приміщення:

$$n = (E \cdot S \cdot Z \cdot k)/(F \cdot U \cdot M), \quad (5.6)$$

Отже, $n = (200 \cdot 120 \cdot 1{,}2 \cdot 1{,}5)/(3120 \cdot 0{,}6 \cdot 2) = 12$.

Виходячи з цього, рекомендується використовувати 12 світильників. Світильники слід розміщувати рядами, бажано паралельно стіні з вікнами. Схема розташування світильників зображена на рис. 4.1.

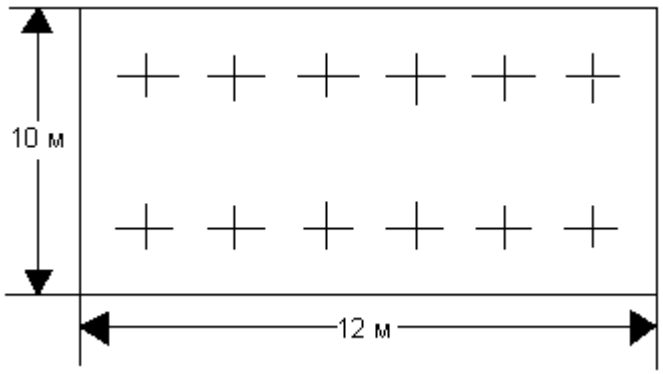


Рисунок 5.1 - Схема розташування світильників

5.4 Рекомендації по пожежній безпеці

Пожежі в приміщеннях, де встановлена обчислювальна техніка, представляють небезпеку для життя людини. Пожежі також пов’язані як з матеріальними втратами, так і з відмовою засобів обчислювальної техніки, що у свою чергу спричиняє за собою порушення ходу технологічного процесу.

Пожежа може виникнути при наявності горючої речовини та внесення джерела запалювання в горюче середовище. Пальними матеріалами в приміщеннях, де розташовані ПЕОМ, є:

– поліамід - матеріал корпусу мікросхеми, горюча речовина, температура самозаймання аерогелю 420 З ;

– полівінілхлорид - ізоляційний матеріал, горюча речовина, температура запалювання 335 З, температура самозаймання 530 З, кількість енергії, що виділяється при згоранні - 18000 - 20700 кДж/кг;

– стеклотекстоліт ДЦ - матеріал друкарських плат, важкозаймистий матеріал, показник горючості 1.74, не схильний до температурного самозаймання;

– пластика кабельний №489 - матеріал ізоляції кабелю, горючий матеріал, показник горючості більш 2.1;

– деревина - будівельний і обробний матеріал, матеріал з якого виготовлені меблі, горючий матеріал, показник горючості більше 2.1, теплота згорання 18731 - 20853 кДж/кг, температура запалювання 399 З, схильна до самозаймання [56].

Згідно [57] приміщення відносяться до категорії В(пожежовибухонебезпечним) і згідно правилам побудови електроустановок простір усередині приміщення відноситься до вогненебезпечної зони класу П - IIа (зони, розташовані в приміщеннях, в яких зберігаються тверді горючі речовини).

Потенційними джерелами запалення при роботі ПЕОМ є:

– іскри при замиканні і розмиканні ланцюгів;

– іскри і дуги коротких замикань;

– перегріви від тривалого перевантаження і наявності перехідного опору.

Продуктами згорання, що виділяються при пожежі, є : оксид вуглецю, сірчистий газ, оксид азоту, синильна кислота, акропеін, фосген, хлор та ін. При горінні пластмас, окрім звичайних продуктів згорання, виділяються різні продукти термічного розкладання: хлорангідрідні кислоти, формальдегіди, хлористий водень, фосген, синильна кислота, аміак, фенол, ацетон, стирол та ін., що шкідливо впливають на організм людини.

Для захисту персоналу від дії небезпечних і шкідливих чинників пожежі проектом передбачається застосування промислового протигаза з коробкою марки В(жовта).

Пожежна безпека об’єктів народного господарства регламентується [58] і забезпечується системами запобігання пожежам і протипожежному захисту. Для успішного гасіння пожеж вирішальне значення має швидке виявлення пожежі і своєчасний виклик пожежних підрозділів до місця пожежі.

Зменшити горюче навантаження не представляється можливим, тому проектом передбачається застосувати наступні способи і їх комбінації для запобігання утворенню(внесення) джерел запалення :

– застосування устаткування, що задовольняє вимогам електростатичної безпеки;

– застосування в конструкції швидкодіючих засобів захисного відключення можливих джерел запалення;

– виключення можливості появи іскрового заряду статичної електрики в горючому середовищі з енергією, рівної і вище мінімальної енергії запалення;

– підтримка температури нагріву поверхні машин, механізмів, устаткування, пристроїв, речовин і матеріалів, які можуть увійти до контакту з пальним середовищем, нижче гранично допустимої, становить 80% якнайменшої температури самозаймання пального.

– заміна небезпечних технологічних операцій більш безпечними;

– ізольоване розташування небезпечних технологічних установок і устаткування;

– зменшення кількості пальних і вибухонебезпечних речовин, що знаходяться у виробничих приміщеннях;

– запобігання можливості утворення пальних сумішей на лінії, вентиляційних системах і ін.;

– механізація, автоматизація та справність(потокова) виробництва;

– суворе дотримання стандартів і точне виконання встановленого технологічного режиму;

– запобігання можливості появи в небезпечних місцях джерел запалення;

– запобігання розповсюдженню пожеж і вибухів;

– використовування устаткування і пристроїв, при роботі яких не виникає джерел запалення;

– виконання вимог сумісного зберігання речовин і матеріалів;

– наявність громовідводу;

– організація автоматичного контролю параметрів, що визначають джерела запалення;

– ліквідація можливості самозаймання речовин і матеріалів .

– Для запобігання пожежі в обчислювальних центрах проектом пропонується виконання наступних вимог :

– електроживлення ЕОМ повинно мати автоматичне блокування відключення електроенергії на випадок зупинки системи охолоджування і кондиціонування;

– система вентиляції обчислювальних центрів повинна бути обладнана блокуючими пристроями, що забезпечують її відключення на випадок пожежі;

– робочі місця повинні бути оснащені пожежними щитами, сигналізацією, засобами для сповіщення про пожежну небезпеку (телефонами), медичними аптечками для надання першої медичної допомоги, розробленим планом евакуації.

Для зниження пожежної небезпеки в приміщеннях використовуються первинні засоби гасіння пожеж, а також система автоматичної пожежної сигналізації, яка дозволяє знайти початкову стадію загоряння, швидко і точно оповістити службу пожежної охорони про час і місце виникнення пожежі.

Відповідно до [59] приміщення категорії В підлягають устаткуванню системами автоматичної пожежної сигналізації. Проектом передбачається застосування датчика типу ІДФ - 1(димовий фотоелектричний датчик), оскільки специфікою пожеж обчислювальної техніки і радіоапаратури є, в першу чергу, виділення диму, а потім - підвищення температури.

При виникненні пожежі в робочому приміщенні обслуговуючий персонал зобов'язаний негайно вжити заходи по ліквідації пожежі. Для ліквідації пожежі використовують вогнегасники (хімічно-пінні, пінні для повітря ОП-5, ОП-6, ОП-9, вуглекислотні ОУ-5), пісок, пожежний інвентар(сокири, ломи, багри, шерстяну або азбестову ковдри) [60]. Як засіб індивідуального захисту проектом передбачається використовування промислового протигаза з маскою, фільтруючої коробки В.

В якості організаційно-технічних заходів рекомендується проводити навчання робочого персоналу правилам пожежної безпеки.

5.5 Охорона навколишнього природного середовища

5.5.1 Загальні дані з охорони навколишнього природного середовища

Діяльність за темою магістерської роботи, а саме розробці автоматизованої системи моделювання рівноважного складу впливає на навколишнє природнє середовище і регламентується нормами діючого законодавства [61 - 66].

Основним екологічним аспектом в процесі діяльності за даними спеціальностями є процеси впливу на атмосферне повітря та процеси поводження з відходами, які утворюються, збираються, розміщуються, передаються на відалення (знешкодження), утилізацію, тощо в ІТ галузі.

Вплив на атмосферне повітря при нормальних умовах праці не оказує, бо не має в приміщенні сканерів, принтерів та інших джерел викиду забруднюючих речовин в повітря робочої зони.

В процесі створення/розробки програми на робочому місці виникають процеси поводження з відходами ІТ галузі. Нижче надано перелік відходів, що утворюються в процесі роботи:

- Відпрацьовані люмінесцентні лампи - І клас небезпеки
- Змінні носії інформації - IV клас небезпеки
- Відпрацьовані вогнегасники - IV клас небезпеки
- Макулатура - IV клас небезпеки
- Відпрацьовані фільтрувальні засоби індивід. захисту (респіратори, протигази) - IV клас небезпеки
- Побутові відходи - IV клас небезпеки

5.5.2 Вимоги до збору, пакування та розміщення відходів ІТ галузі

Наводяться вимоги зберігання виявлених за своєю роботою відходів відповідно до вимог Державних санітарних правил і норм [67].

Відходи в міру їх накопичення збирають у тару, відповідну класу небезпеки, з дотриманням правил безпеки, після чого доставляють до місця тимчасового зберігання відходів відповідно до затвердженої схеми їх розміщення Зазначені для зберігання відходів місця чи об'єкти повинні використовуватися лише для заявлених відходів.

Не допускається зберігання відходів у невстановлених схемою місцях, а також перевищення норм тимчасового зберігання відходів.

Способи тимчасового зберігання відходів визначаються видом, агрегатним станом і класом небезпеки відходів:

- Відходи I класу небезпеки зберігаються в герметичній тарі (сталеві бочки, контейнери). У міру наповнення тару з відходами закривають герметично сталевий кришкою;

- Відходи IV класу небезпеки можуть зберігатися відкрито на промисловому майданчику у вигляді конусоподібної купи, звідки їх автонавантажувачем перевантажують у самоскид і доставляють на місце утилізації або захоронення;

Не допускається змішування відходів різних видів і класів небезпеки.

Особливий контроль наділяється збору і зберіганню відпрацьованих ртутьвмісних ламп (енергоощадних) як відходам I класу небезпеки, що збираються і обов'язково передаються на утилізацію підприємствам, що мають ліцензію на поводження з такими небезпечними відходами.

Всі відходи, що утворюються в процесі діяльності/роботи, підлягають обліку.

Побутові та будівельні відходи вивозяться на полігон твердих побутових відходів міста, також відповідно до договору з комунальним дорожньо-експлуатаційним управлінням.

Особи, винні в порушенні встановленого порядку поводження з відходами (порушення правил обліку відходів, самовільне складування і видалення відходів, передача відходів в інші підприємства/організації з порушенням встановлених правил), згідно законодавства несуть дисциплінарну, адміністративну або кримінальну відповідальність.

5.5.3 Визначення впливу та заходів щодо поводження з відходами IT галузі

З метою визначення та прогнозування впливу відходів на навколишне середовище, своєчасного виявлення негативних наслідків, їх запобігання відповідно до Закону України «Про відходи» повинен здійснюватися моніторинг місць утворення, зберігання, і видалення відходів. Відомості про місце утворення та місце розташування відходів зазначаються на «План схемі місці розміщення відходів організації / виробництва» та наводяться у таблиці 5.2.

Таблиця 5.2 - Відомості про місце утворення та місце розташування відходів

№ з/п	Код та найменування відходів за ДК -005-96	Технологічний процес або виробництво, де утворюються відходи / клас небезпеки	Місце розташування відходу, тара та її кількість, місткість, розміри у разі наявності майданчиків розташування відходів необхідно зазначити тип покриття та наявність даху)	№ на схемі (додається масштабна схема місць розміщення відходів)
1	7710.3.1.26 Лампи люмінесцентні, та відходи, які містять ртуть, інші зіпсовані або відпрацьовані (Відпрацьовані ртутьвмісні люмінесцентні лампи)	1	буд.84, в приміщені кладової S=100м^2, в кількість 50 од.	8401-ТХ
2	7720.3.1.01 Відходи комунальні (міські) змішані, у т.ч. сміття з урн (Побутові відходи)	4	зовнішній майданчик зберігання побутових відходів біля буд .84 S=5м² V= 2,08м³- 2од.	8401-ТХ
3	7710.3.1.01 Макулатура паперова та картонна (Макулатура)		буд .84 4 поверх в кім. 412 S =5,0 м.^{2}	8401-ТХ
4	8530.2.9.03 Засоби захисту від хімічних або бактеріальних аерозолів зіпсовані, або відпрацьовані (Відпрацьовані фільтрувальні засоби індивідуального захисту)	4	буд .84- 1 поверх кладова S=2м² V= 0,64м³- 1од.	8401-ТХ
5	Змінні носії інформації	4	буд. 84, кім. 412 V=0,0005 м^3	8401-ТХ

Відомості про склад і властивості відходів, що утворюються, а також ступінь їх небезпечності для навколишнього природного середовища та здоров'я людини у табл. 5.3.

Таблиця 5.3 – Відомості про склад і властивості відходів, що утворюються, а також ступінь їх небезпечності для навколишнього природного середовища та здоров'я людини

№ п/п	Назва відходу	Клас небезпечності	Хімічний (у долях відсотків складників або інших одиницях виміру) та морфологічний склад	Фізико-хімічні властивості	Негативний вплив на навколишнє середовище та здоров'я людини
1	2	3	4	5	6
1	Відпрацьовані люмінесцентні лампи	I	**Ртуть** - 0,013 **Hg** **Скло** - 98,787 **$(Na, K)_2 O\ 2SiO_2$** **Алюміній** - 1,2 **Al**	**Ртуть** - $T_{кип.}$ = 356,58°C $T_{плав.}$ = **-38,87°C** **Скло** - $T_{плав.}$ = 800°C **Алюміній** - $T_{кип.}$ = 2348°C $T_{плав.}$ = 660,1°C	Негативний вплив на ОС і людини визначається його хімічним складом. **Ртуть** У природних водах міститься в концентрації 0,00003 ... 0,0028 мг / л. Являючись потужним кумулятивним отрутою, з можливою канцерогенною і мутагенною дією. Процеси самоочищення водойм порушують концентрація ртуті понад 0,018 мг / л, порогова концентрація ртуті за впливом на санітарний режим водойм-0,01 мг / л. Наприкінці концентрація понад 0,03 є токсичною практично для всіх видів водних організмів. Надзвичайно токсична при попаданні з питною водою для тепло-кровних організмів, надходження ртуті з питною водою в кількості 75,0 ... 300,0 мг / сут є смертельним. Відрізняється високою токсичністю для будь-яких форм життя. При отруєнні па-рами спостерігається слабкість, головний біль, біль в шлунку, роздратування по-чек, навіть нефрит; катаральні явища. Розвивається тремтіння рук, ніг, всього тіла. Виникає стан підвищеної психічної збудливості. Пари ртуті проявляють нейротоксичність, особливо страждають вищі відділи нервової системи

Продовження табл. 5.3

1	2	3	4	5	6
					Скло Нетоксичні, безпечно в навколишньому середовищу, не шкідлива в нирках і водоймах. Вдихання скляного пилу (волокон) призводить до силікоз в зв'язку з високим вмістом сполук кремнію. Шкідливої дії не робить, але є небезпека механічних пошкоджень (порізи, травми). **Алюміній** Токсичний для водної біоти, теплокровних тварин і людей, в концентрації> 1 мг / л чинить негативний впливав на зростання с /г культур. У концентрації> 1 мг / л гальмує зростання мікрофлори водойм і стримує процеси самоочищення водойм. Рівень токсичності визначається формою, в якій знаходиться елемент. Впливає на обмін речовин і функції нервової системи. При попаданні на ґрунт, в воду і атмосферними повітря надає негативного впливу на НС і здоров'я людини.
5	Макулатура	IV	**Цинк** - 0,000053 – 0,000056 **Zn** **Свинець** - 0,000049 – 0,000051 **Pb**	Уривки та обрізки з паперових мішків **Цинк** $T_{кип.}$= 913°C $T_{плав.}$= 4,19°C **Свинець** $T_{кип.}$= 1751°C $T_{плав.}$= 327,3°C	Негативний вплив на ОС і людини визначається його хімічним складом. **Цинк** Малотоксичний для теплокровних тварин при надходженні з їжею і питної водою-концентрація в питній воді 11,2 ... 26,6 мг / л переноситься без будь-яких ознак інтоксикації. Дуже корисний для флори, будучи одним з найважливіших мікроелементів харчування, однак лише в концентрації до 0,2 мг / л, крім того, елемент силяється до кумуляції в грантах. Дуже токсичний для водних організмів, порушуючи процеси самоочищення водойм і стаючи токсичним для іхтіофауни в концентрації 0,15 ... 5,0 мг / л. **свинець** У природних водах міститься в концентрації 0,001 - 0,023 мг / л. У концентрації 2,0 мг / л надає воді металевий присмак. Можливо має мутагенну і канцерогенну дію, значно збільшує токсичну дію інших металів. В конценрації 1,90 мг / л згубно діє на дафній, концентрація 0,1 мг / л погіршує процеси самоочищення водойм. Свинець токсичний для рослин в концентрації понад 5,0 мг/кг ґрунту.

Продовження табл. 5.3

1	2	3	4	5	6
			Хром - 0,000051 – 0,000054 **Cr** **Мідь** - 0,000033 – 0,000035 **Cu** **Целюлоза** - 97,299814 – 96,999804 **$(C_6H_{10}O_5)_n$** **Вода** - 2,7 – 3,0	**Хром** $T_{кип.}$= 1890°C $T_{плав.}$= 2480°C **Мідь** $T_{кип.}$= 2580°C $T_{плав.}$= 1083°C **Целюлоза** $T_{возг. с обуглив.}$ ≥ 100°C	Помірно токсичний. Викликає хронічне отруєння. Має здатність вражати центральну і периферичну нервову систему, кістковий мозок і кров, судини, синтез білка, генетичний апарат клітини. **хром** Міститься в природних водах в концентрації 0,001 ... 0,112 мг / л. LK50 Cr (VI) для риб-30,0 ... 50,0 мг / л, LK50 Cr (III) для риб- 117,0 мг / л. Низькі концентрації хрому позитивно впливають на ріст рослин, проте полив водою С / Г культур з концентрацією хрому 10,0 ... 50,0 мг / л гальмує їх розвиток. На тварин надає загально токсичне, подразнююче, кумулятивне, алергенну, канцерогенну і мутагенну дію. Володіє канцерогенними властивістю (2) **мідь** У природних водах міститься в концентраціях 0,001 ... 0,98 мг / л. У концентрації 0,5 мг / л забарвлює воду, в концентрації> 1,0 мг / л-помітно збільшує мутність води. Дуже токсична як для водних організмів, так і для рослин. У концентрації 0,001 мг / л гальмує розвиток синьо зелених водоростей, LK50 практично для всіх видів риб становить 0,18 ... 1,35 мг / л (короп, карась, окунь, щука, сом). Куммулюється ґрунтом і рослин-ями. У концентрації 0,1 ... 0,2 мг / л надає токсичну дію на ріст рослин. Високотоксичний метал. Викликає гостре отруєний-ня, має широкий спектр токсичної дії (2) **целюлоза** Нетоксична. Досить легко підвержен біодеструкції лігнін- і целюлозоруйнуючими бактеріями і деякими класами низших грибів. У зв'язку з нетоксичністю LD50 для тваринах не установлена. Токсичність визначається за вмістом важких металів, здатних мігрувати з неї в навколишнє середовище. При попаданні на ґрунт, в воду і атмосферне повітря чинить негативний вплив на ОС і здоров'я людини.

Продовження табл. 5.3

1	2	3	4	5	6
9	**Побутові відходи**	IV	Побутові відходи - 100 – 100, в т. ч.: Папір - 30 - 17; [$(C_6H_{10}O_5)_n$ - целюлоза] Поліетилен -20 – 24; **(- CH_2 - CH_2 -)$_n$** Деревина -5 – 3; [$(C_6H_{10}O_5)_n$ - целюлоза, лігнін] Матеріали текстильні -4 – 3; [$(C_6H_{10}O_5)_n$ - целюлоза	Целюлоза $T_{возг. с обуглив.} \geq 100°C$ Поліетилен - $T_{размяг.} \geq 150°C$ Твердий матеріал рослинного походження, не розчиняється у воді. Целюлоза, лігнін $T_{возг. с обуглив.} \geq 120°C$ Твердий матеріал рослинного походження, не розчиняється у воді. Целюлоза	Негативний вплив на ОС і людини визначається його хімічним складом. **целюлоза** Нетоксична. Досить легко піддавав біодеструкції лігнін- і целюлозоруйнуючими бактеріями і деякими класами низших грибів. У зв'язку з нетоксичністю LD50 для тваринах не установлена. Токсичність визначається за вмістом важких металів, здатних мігрувати з неї в навколишнє середовище **поліетилен** Нетоксичний для всіх видів флори і фауни в зв'язку з дуже високою біологічною інертністю. Нерозчинний у водних середовищах і не впливає на санітарний режим водойм. Використання його не вимагає запобіжних заходів. Отруєння можливі при виробництві та переробці плівки, в результаті виділення окису вуглецю, альдегідів, органічних кислот [45] **деревина** Нетоксична. Досить легко піддається біодеструкції лігнін- і целюлозоруйнуючими бактеріями і деякими класами нижчих грибів. У зв'язку з нетоксичністю LD50 для тварин не встановлена. Деревина нетоксична при використання. Але дія деревного пилу при рубці і переробці деревини викликає захворювання дихальних шляхів і шкіри. текстильне волокно Нетоксична в зв'язку з біогенним походженням, проте для біодеструкції необхідна наявність вологи. Нетоксична при використанні. Токсична дія виникає (як результат механічні дії -наслідок пилу) при виробництві тканів і при переробці вторинних матеріалів; слабкий алерген.

Продовження табл. 5.3

1	2	3	4	5	6
			Мінеральні домішки (пісок, глина) -4 – 9 Харчові відходи -37 –44;	$T_{возг.\ с\ обуглив.} \geq 100°C$ Харчові відходи $T_{биоразл.} \geq 4°\ C$	**Глина** нетоксична нетоксична

У розділі «Охорона праці та безпека в надзвичайних ситуаціях» виконано аналіз потенційних небезпек при роботі із засобами обчислювальної техніки і механізмами, розроблені заходи щодо техніки безпеки, заходи, які забезпечують виробничу санітарію і гігієну праці, розраховане штучне освітлення, виконані рекомендації по пожежній безпеці.

ВИСНОВКИ

З розвитком інтернету речей все більше предметів будуть підключатися до глобальної мережі, тим самим створюючи нові можливості у сфері безпеки та управління, відкриваючи нові перспективи і сприяючи підвищенню якості життя населення.

На сьогоднішній день, на підставі технології Інтернету речей вже функціонують такі системи, як розумний будинок, смарт офіс і смарт білдінг. Ідея цих розумних будівель полягає в тому, щоб створити єдиний центр управління інженерними системами будівлі з автоматичним встановленням оптимальних режимів. Реалізація такої концепції дозволить вирішити проблеми енергозбереження і відповідно економії коштів, спрямованих на експлуатацію будівлі. Найбільш доцільно застосовувати концепцію інтелектуальної будівлі у проектах, призначених для бізнесу – це офіси та готелі, а також освітні установи та ін.

Всі системи розумного будинку вирішують три основні завдання: комфорт, безпека, економічність. І саме на це завжди потрібно орієнтуватися при проектуванні інженерної інфраструктури будівлі, монтажу і пуско-наладки.

Що стосується вищого закладу, то багато з описаних вище підходів і принципів поки ще залишаються нереалізованими і можуть розглядатися як мета, як керівництво до дії. У той же час очевидно, що на даному етапі розвитку техніки, технологій, матеріально-технічної та науково-педагогічної бази системи освіти є все можливе для того, щоб в найближчому майбутньому реалізувати цю концепцію і в нашому Східноукраїнському національному університеті ім. В.Даля і скористатися всіма незаперечними перевагами смарт будівлі.

На підставі поставленої мети була запропонована система управління вищим навчальним заклад з використанням технології Інтернету речей, яка дозволить вирішити проблеми енергозбереження та відповідно економити кошти, спрямовані на експлуатацію будівлі.

У розділі «Охорона праці та безпека в надзвичайних ситуаціях» виконано аналіз потенційних небезпек при роботі із засобами обчислювальної техніки і механізмами, розроблені заходи щодо техніки безпеки, заходи, які забезпечують виробничу санітарію і гігієну праці, розраховане штучне освітлення, виконані рекомендації по пожежній безпеці.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1) Восков Л.С Интернет вещей / Л.С. Восков // "Новые информационные технологии". Тезисы докладов XX Международной студенческой конференции-школы-семинара, М.: МИЭМ, 2012. – с. 89-94.

2) Castalia official site [Электронный ресурс] / Castalia: URL: http://castalia.research.nicta.com.au/

3) Castalia User's manual [Электронный ресурс] / Castalia: URL: http://castalia.research.nicta.com.au/pdfs/Castalia%20-%20User%20Manual.pdf

4) Chandra T.D., Toueg S. Unreliable failure detectors for reliable distributed systems. // J. ACM. 1996. V. 43. P. 225-267.

5) Delporte-Gallet C., Devismes S., Fauconnier H. Stabilizing leader election in partial synchronous systems with crash failures. // J. Parallel Distrib. Comput. - 2010. - 70. - P. 45 - 58.

6) E. Egea-Lpez, J. Vales-Alonso, AS Martnez-Sala, P. Pavn-Mario, J. Garca-Haro Simulation Tools for Wireless Sensor Networks // Summer Simulation Multiconference - SPECTS 2005 // - 2005. - P. 2 - 9.

7) Ezio Biglieri Coding for Wireless Channels (Information Technology: Transmission, Processing and Storage) -2005. - P. 428.

8) Fei Yu A Survey of Wireless Sensor Network Simulation Tools URL: http://www1.cse.wustl.edu/~jain/cse567-11/ftp/sensor/index.html

9) Fischer MJ, Lynch NA, Paterson MS Impossibility of distributed consensus with one faulty process. // J. ACM. 1985. V 32. P. 374-382.

10) Garay JA, Perry KJ A continuum of failure models for distributed computing. // Proc. 6nd Int. Workshop on Distributed Algorithms (Haifa, 1992) / S. Zaks, A. Segall (eds.). P. 153-156.

11) IEEE Standards 802.15.4. Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs). - IEEE Computer Society, 2003.

12) Luis Javier Garca Villalba, Ana Lucila Sandoval Orozco, Alicia Trivio Cabrera, Cludia Jacy Barenco Abbas Routing Protocols in Wireless Sensor Networks // Sensors // - 2009 - 9 - P. 399-421.

13) Pease M., Shostak R., Lamport L. Reaching agreement in the presence of faults. // J. ACM. 1984. V. 27. P. 228-234.

14) Roya N., Gub T., Das SK Supporting pervasive computing applications with active context fusion and semantic context delivery. // Pervasive and Mobile Computing - 2010. - 6. - P. 21-42.

15) Zhang M., Chan MC, Ananda AL Connectivity monitoring in wireless sensor networks. // Pervasive and Mobile Computing - 2010 року.- 6. - P. 112-127.

16) Акімов О.В., Кузнєцов М.Н. Імовірнісні математичні моделі для оцінки надійності бездротових сенсорних мереж // Електронний журнал «Праці МАІ». Випуск № 40 // URL: http://www.mai.ru/science/trudy/

17) Ахо А., Хопкрофта Д., Ульман Д. Структури даних і алгоритми / А. Ахо - М .: Вільямс, 2000. - 384 с.

18) Гейер Д.Ж. Бездротові мережі. Перший крок. // Пер. з англ. / Д.Ж. Гейер - М .: Вільямс, 2005. - 192 с.

19) Нечаєв Д.Ю., Чекмарьов Ю.В. Надійність інформаційних систем / Д.Ю.. Нечаєв - М .: ДМК Пресс, 2012. - 64 с.

20) Острейковский В.А. Теория надежности / В.А Острейковский М.: Высшая школа, 2000. − 464 с.

21) Острейковский В.А. Теория надежности. Учебник для ВУЗов / В.А Острейковский − М.: Высшая школа, 2003. − 457 с.

22) Половко А.М., Гуров С. В. Основы теории надежности / А.М. Половко − СПб.: БХВ-Петербург 2006. − 560 с.

23) Смелянский Р. Л. Компьютерные сети. В 2 томах. Том 1. Системы передачи данных / Р.Л Смелянский − М.: Академия, 2011. − 304 с.

24) Тель Ж. Введение в распределенные алгоритмы. Пер. с англ. В. А. Захарова. / Ж. Тель − М.: МЦНМО, 2009. − 616 с.

25) Ушаков И.А. Вероятностные модели надежности информационно-вычислительных систем. / И.А Ушаков − М.: Радио и связь 1991. − 132 с.

26) Хьюз К., Хьюз Т. Параллельное и распределенное программирование на C++. Пер. с англ. / К. Хьюз − М.: Издательский дом Вильямс, 2004. − 672 с.

27) Шахнович И.А.Современные технологии беспроводной связи. /И.А Шахнович − М.: Техносфера, 2006. − 288 с.

28) Шубин В.И. Беспроводные сети передачи данных / В.И. Шубин, О. С. Красильникова. − М.: ВУЗовская книга, 2012. − 104 с.

29) Эндрюс Г.Р. Основы многопоточного, параллельного и распределенного программирования / Г.Р. Эндрюс // Пер. с англ. − М.: Издательский дом Вильямс, 2003. − 512 с.

30) Вабищевич А. Н. Определение положения в пространстве элементов бес проводной сенсорной сети с помощью инерциальных сенсоров / А.Н. Вабищевич // Тезисы докладов научно-технической конференции студентов, аспирантов и молодых специалистов МИЭМ’2010. − М.: МИЭМ, 2010. − С. 151-152.

31) Васильев Ф. П. Численные методы решения экстремальных задач: Учеб. пособие для ВУЗов. − 2-е изд., перераб. и доп. / Ф.П Васильев − М.: Наука, 1988. 552 с.

32) Вишневский В. М. Широкополосные беспроводные сети передачи информации / В.М. Вишневский − М.: Техносфера, 2005. 592 с.

33) Гекк М. В., Истомин Т. Е., Файзулхаков Я. Р., Чечендаев А. В. Адаптивный алгоритм быстрой доставки сообщений по выделенным направлениям для беспроводных сетей датчиков / М.В. Гекк // Вестник молодых ученых "Ломоносов". Выпуск III. 2006. С. 55–60.

34) Ефремов В. В., Маркман Г. З. "Энергосбережение"и "энергоэффективность": уточнение понятий, система сбалансированных показателей энергоэффективности / В.В. Ефимов // Известия Томского политехнического университета. 2007. Т. 311, No 4. С. 146–148.

35) Ефремов С. Г. Разработка системы активного беспроводного сбора данных в интралогистике (номер государственной регистрации НИОКР01200961253).

36) Жданов В. С. Проблемы и задачи проектирования беспроводных сенсорных сетей // Информационные, сетевые и телекоммуникационные технологии: сборник научных трудов, под ред. проф. д.т.н. Жданова В.С. 2009. С. 8–21.

37) Иванов Е. В. Определение координат в беспроводных сенсорных сетях: дис. канд. техн. наук: 05.12.13. 2008. 149 с.

38) Комаров М. М. Разработка и исследование метода энергетической балансировки беспроводной стационарной сенсорной сети с автономными источниками питания: дис. ... канд. техн. наук: 05.12.13. 2012. 125 с.

39) Комаров М. М., Восков Л. С. Позиционирование датчиков беспроводной сети как способ энергосбережения // Датчики и системы. 2012. Т. 1. С. 34–38.

40) Курпатов Р. О. Исследование и разработка энергоэффективного метода локализации элементов беспроводных сенсорных сетей: дис. ... канд. техн. наук: 05.12.13. М., 2011. 126 с.

41) Оліфер В. Г., Оліфер Н. А. Комп'ютерні мережі. Принципи, технології, протоколи. СПб .: Пітер, 4-е видання, 2010. 943 с.

42) Юркін В. Ю., Мохсені Т. І. Ієрархічні підходи до самоорганізації в бездротових широкосмугових сенсорних мережах на основі хаотичних радиоимпульсов // Праці МФТІ. 2012. Т. 4, No 3. С. 151-161.

43) Кулаков В. Справочник по шаблонам проектирования [Электронный ресурс] / В. Кулаков. – Режим доступа: http://design-pattern.ru/patterns/mvc.html . – Дата доступа: 22.01.2017. – Загл. с экр.

44) Определение шаблона MVVM [Електронный ресурс] . – Режим доступа: http://metanit.com/sharp/wpf/22.1.php . – Дата доступа: 22.01.2017. – Загл. с экр.

45) Redux Official Documentation [Електронный ресурс]. – Режим доступа: https://docs.reduxframework.com . – Дата доступа: 22.01.2017. – Загл. с экр.

46) ГОСТ 12.1.005-88. Общие санитарно-гигиенические требования к воздуху рабочей зоны.

47) ГОСТ 12.0.003-74 Опасные и вредные производственные факторы. Классификация.

48) НПАОП 40.1-1.21-98. Правила безпечної експлуатації електроустановок споживачів

49) ГОСТ 12.1.009-76. ССБТ. Электробезопасность. Термины и определения.

50) *СН 245-71* (ДНАОП 0.03-3.01-71) Санитарные нормы проектирования промышленных предприятий

51) ДСН 3.3.6.042-99 Санітарні норми мікроклімату виробничих приміщень.

52) ГОСТ 12.1.005-88. Система стандартов безопасности труда. Общие санитарно-гигиенические требования к воздуху рабочей зоны.

53) TCO’ 07 Certified Displays. © 2007 Copyright TCO Development AB

54) ДСанПіН 3.3.2.007-98, Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин.

55) ДБН В.2.5-28-2006. Природне і штучне освітлення

56) ГОСТ 12.1.044-89 Система стандартов безопасности труда. Пожаровзрывоопасность веществ и материалов. Номенклатура показателей и методы их определения.

57) НАПБ Б.03.002-2007. Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою.

58) ГОСТ 12.1.004-91. "Система стандартов безопасности труда. Пожарная безопасность. Общие требования".

59) НАПБ А.01.001-2014 “Правила пожежної безпеки в Україні”

60) НАПБ Б.03.001-2004. Про затвердження Типових норм належності вогнегасників.

61) Закон України «Про охорону навколишнього природного середовища»

62) Закон України «Про забезпечення санітарного та епідемічного благополуччя населення»

63) Закон України «Про відходи»

64) Закон України «Про охорону атмосферного повітря»

65) Закон України «Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру»

66) Водний кодекс України

67) ДСанПіН 2.2.7.029-99. Гігієнічні вимоги щодо поводження з промисловими відходами та визначення їх класу небезпеки для здоров'я населення.

ДОДАТОК А.
Лістинг файлів скриптів

Index.html

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
   <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
   <title>Temperatura 1-wire DS18B20</title>
   <script type="text/javascript" src="/webiopi.js"></script>
   <script type="text/javascript">

      // Вызов макроса изменения температуры с интервалом 5 сек.
            setInterval ("callMacro_getTmp0()", 5000);{
            }
       // Запрос температуры
            function callMacro_getTmp0(){
            webiopi().callMacro("getTmp0", [], macro_getTmp0_Callback);
             }
      // Получение температуры
            function macro_getTmp0_Callback(macro, args, data) {
            $("#celsius_0").text("Температура: "+data+" °C");
            }
setInterval ("callMacro_tihour()", 2000);{
}
function callMacro_tihour(){
webiopi().callMacro("tihour", [], macro_tihour_Callback);
}
function macro_tihour_Callback(macro, args, data) {
$("#hr").text(data);
}
   webiopi().ready(function() {
  // Following function will process data received from set/getLightHours macro.
      var updateLightHours = function(macro, args, response) {
               var hours = response.split(";");
               // Following lines use jQuery functions
               $("#inputOn").val(hours[0]);
               $("#inputOff").val(hours[1]);
                $("#inputOnm").val(hours[2]);
                $("#inputOffm").val(hours[3]);
      }
// Immediately call getLightHours macro to update the UI with current values
// "getLightHours" refers to macro name
// [] is an empty array, because getLightHours macro does not take any argument
// updateLightHours is the callback function, defined above

            webiopi().callMacro("getLightHours", [], updateLightHours);

      // Create a button to call setLightHours macro
```

```
  var sendButton = webiopi().createButton("sendButton", "Передать", function() {
        // Arguments sent to the macro
  var hours = [$("#inputOn").val(), $("#inputOff").val(), $("#inputOnm").val(),
$("#inputOffm").val()];
          // Call the macro
            webiopi().callMacro("setLightHours", hours, updateLightHours);
             });

      // Append the button to the controls box using a jQuery function
            $("#send_contr").append(sendButton);

      // Create a "Обогреватель" labeled button for GPIO 23
      var button = webiopi().createGPIOButton(23, "Обогреватель");

      // Append button to HTML element with ID="controls" using jQuery
      $("#controls").append(button);

      // Create a "Розетка 1" labeled button1 for GPIO 9
      var button1 = webiopi().createGPIOButton(9, "Розетка ");

      // Append button to HTML element with ID="controls1" using jQuery
      $("#controls1").append(button1);

      // Refresh GPIO buttons
      // pass true to refresh repeatedly of false to refresh once
            webiopi().refreshGPIO(true);
   });
   </script>


      }
      #gpio23.LOW {
         background-color: Green;
      }
      #gpio23.HIGH {
         background-color: Black;
      }
      #gpio9.LOW {
         background-color: green;
      }
      #gpio9.HIGH {
         background-color: black;
      }
      }
   </style>
</head>
<body>
<div align="center">
  Включить обогреватель, часы, минуты:<input type="text" maxlength="2"
size="2" id="inputOn" />
<input type="text" maxlength="2" size="2" id="inputOnm" /><br/>
```

```
Выключить обогреватель, часы, минуты:<input type="text" maxlength="2" size="2" id="inputOff" />
<input type="text" maxlength="2" size="2" id="inputOffm" /><br/>
</div>
<div align="center">
   <div id="send_contr" align="center"></div>
   <div id="hr" align="center"></div>
   <div id="controls" align="center"></div>
   <div id="controls1" align="center"></div>
   <div id="controls2" align="center"></div>
   <div id="celsius_0" align="center"></div>
</div>
<center><FONT color="#008000"><FONT size="5">График изменения температуры:<br></FONT></FONT></center>
<a href="temp.html" target="_blank"><center><FONT size="5">1. Кафедра КСМ <br></FONT></center></a>
</body>
</html>
```

Script.py

```
import webiopi
import datetime
import time
from webiopi import deviceInstance
from time import strftime
GPIO = webiopi.GPIO

LIGHT = 23 # GPIO pin

HOUR_ON  = 0  # Turn Light ON at 13:00
HOUR_OFF = 0  # Turn Light OFF at 14:00
MIN_ON = 0
MIN_OFF = 0
celsius_0 = 0,0
cel_0=0,0
num=1
# setup function is automatically called at WebIOPi startup
def setup():
   # set the GPIO used by the light to output
   GPIO.setFunction(LIGHT, GPIO.OUT)

   # retrieve current datetime
   now = datetime.datetime.now()
   # test if we are between ON time and tun the light ON
   if (((now.hour >= HOUR_ON) and (now.hour <= HOUR_OFF)) and ((now.minute >= MIN_ON) and (now.minute <= MIN_OFF))):
      GPIO.digitalWrite(LIGHT, GPIO.LOW)

@webiopi.macro
def getTmp0():
   global celsius_0
```

```
    tmp0 = webiopi.deviceInstance("tmp0")
    celsius_0 = tmp0.getCelsius()  # получение температуры
    print (celsius_0)
    return "%.2f" % celsius_0 # возврат данных температуры в HTML
    # с округлением до сотых

@webiopi.macro
def tihour():
    now = datetime.datetime.now()
    return "Время {0}, {1}".format("%d:%d %d:%d" % (HOUR_ON, MIN_ON,HOUR_OFF,
MIN_OFF), strftime("%Y-%m-%d %H:%M"))

def loop():
    global cel_0
    global num
   # retrieve current datetime
    now = datetime.datetime.now()
    # toggle light ON all days at the correct time
    if ((now.hour == HOUR_ON) and (now.minute == MIN_ON) and (now.second == 0)):
        if (GPIO.digitalRead(LIGHT) == GPIO.HIGH):
          GPIO.digitalWrite(LIGHT, GPIO.LOW)

    # toggle light OFF
    if ((now.hour == HOUR_OFF) and (now.minute == MIN_OFF) and (now.second == 0)):
        if (GPIO.digitalRead(LIGHT) == GPIO.LOW):
          GPIO.digitalWrite(LIGHT, GPIO.HIGH)
    if (num==300):
      tmp0 = webiopi.deviceInstance("tmp0")
      cel_0 = tmp0.getCelsius()
      f = open('/home/pi/myproject/html/data_18B20.txt', 'a')
      data_entry = "{0},{1}\n".format(strftime("%Y-%m-%d %H:%M:%S"),"%.2f" % cel_0)
      f.write(data_entry)
      f.close()
      num=0
    num+=1
    # gives CPU some time before looping again
    time.sleep(1)

@webiopi.macro
def getLightHours():
    return "%d;%d;%d;%d" % (HOUR_ON, HOUR_OFF, MIN_ON, MIN_OFF)

@webiopi.macro
def setLightHours(on, off, onm, offm):
    global HOUR_ON, HOUR_OFF, MIN_ON, MIN_OFF
    HOUR_ON = int(on)
    HOUR_OFF = int(off)
    MIN_ON = int(onm)
    MIN_OFF = int(offm)
    return getLightHours()

# destroy function is called at WebIOPi shutdown
```

```
def destroy():
    GPIO.digitalWrite(LIGHT, GPIO.HIGH)
```

ДОДАТОК Б.
Електронні плакати

Східноукраїнський національний університет ім.В.Даля

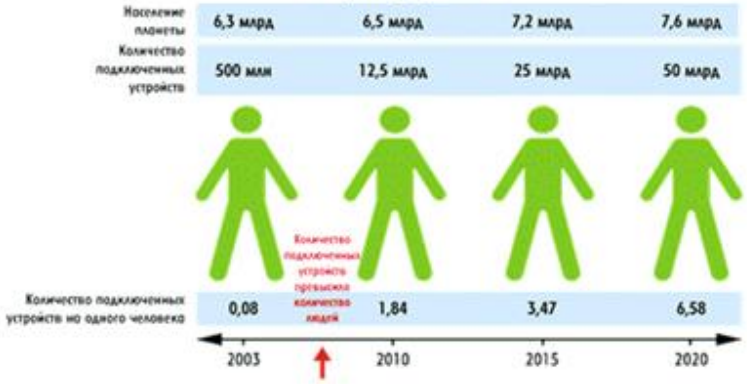
Магістерська робота

«Комп'ютерна система моніторінгу та управління навчальним закладом»

Студент гр.КСМ-16зм
Дерябін І.О.
Керівник:
Барбарук В.М.

Актуальність теми:

Актуальність теми дослідження обумовлена високим потенціалом розвитку технології Інтернету речей

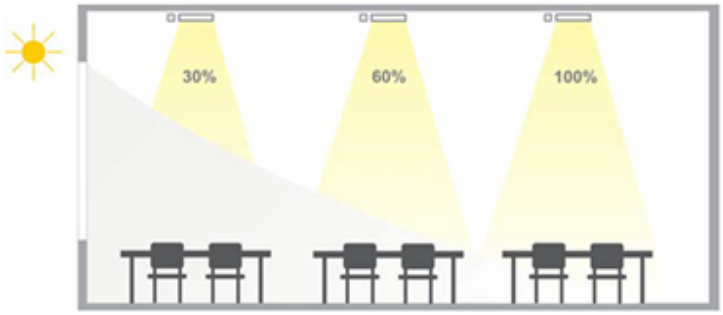


По данным компании Cisco, взрывной рост смартфонов и планшетных компьютеров довел число устройств, подключенных к Интернету, до 12,5 млрд в 2010 году, в то время как число людей, живущих на Земле, увеличилось до 6,8 млрд;

Під Інтернетом речей розуміється сукупність різних приладів, датчиків, пристроїв, об'єднаних в мережу за допомогою будь-яких доступних каналів зв'язку, що використовують різні протоколи взаємодії між собою і єдиний протокол доступу до глобальної мережі. У роботі в якості глобальної мережі для Інтернет речей будемо використовувати мережу Інтернет. Спільним протоколом буде IP.

Технология	Назначение	Базовые характеристики	Организация, занимающаяся стандартизацией и/или продвижением
Bluetooth Low Energy	Персональные сети (PAN)	Низкая пропускная способность, малое энергопотребление	Bluetooth Special Interest Group
Wi-Fi	Локальные сети	Высокая пропускная способность, высокое энергопотребление	IEEE
ZigBee	Локальные сети	Низкая пропускная способность, малое энергопотребление	IEEE
GSM, GPRS, EC-GSM-IoT (EC — Enhanced Coverage)	Территориально распределенные сети (WAN), глобальное покрытие	Недорогие сотовые модемы, низкая пропускная способность	3GPP

Автоматичне управління освітленням аудиторії



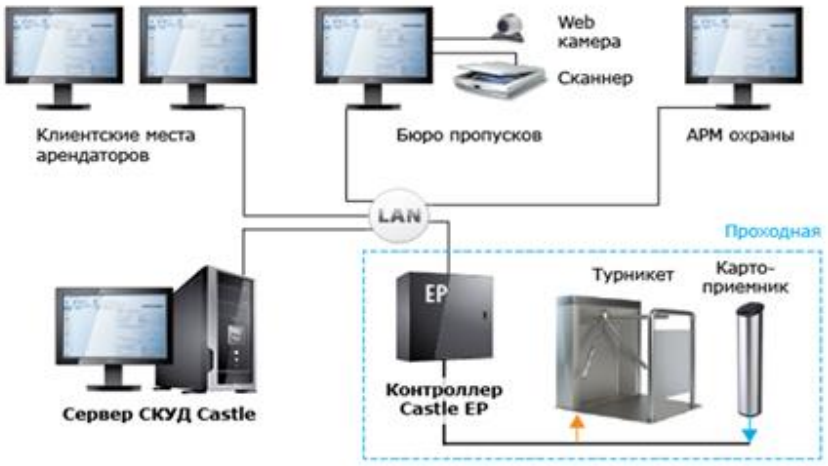
Підвищити ефективність систем освітлення аудиторії можна шляхом установки датчиків постійної освітленості на стелі над кожним рядом парт. Цей датчик здатний підтримувати заданий рівень освітленості, автоматично зменшуючи або збільшуючи світловий потік групи світильників в залежності від рівня сонячного світла, що проникає в аудиторію через вікна. У світлий час доби світильники, розташовані ближче до вікон працюватимуть з меншою потужністю.

Розташування датчиків освітлення в аудиторії

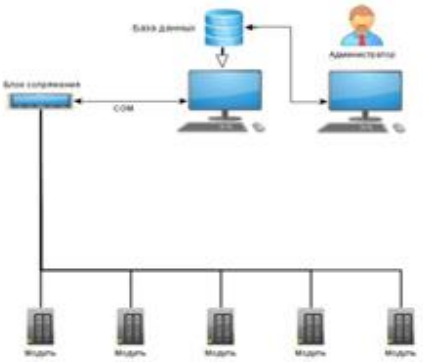
Наочне зображення роботи датчика освітлення

На представленому рисунку наочно видно, як в сонячний день працюють датчики: світильники, розташовані біля вікон, працюють в режимі мінімальної потужності (5% від номінального значення). Другий і третій ряди світильників також працюють в економічних режимах (приблизно 20% і 60% від номінальної потужності відповідно)

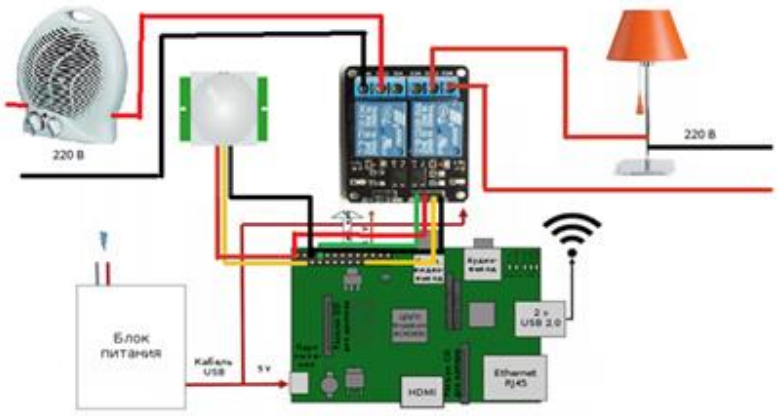
Організації системи контролю доступу

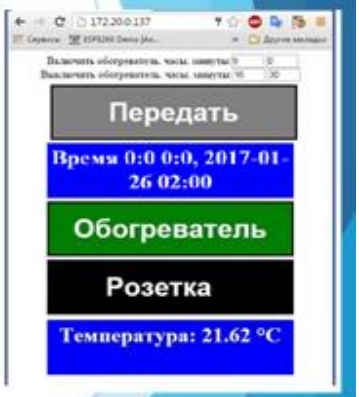


Контроль відвідуваності



Реалізація системи управління і контролю





Результати досліджень

Висновки

Всі системи розумного будинку вирішують три основні завдання: комфорт, безпека, економічність. І саме на це завжди потрібно орієнтуватися при проектуванні інженерної інфраструктури будівлі, монтажу і пуско-наладки.

Що стосується вищого закладу, то багато з описаних вище підходів і принципів поки ще залишаються нереалізованими і можуть розглядатися як мета, як керівництво до дії. У той же час очевидно, що на даному етапі розвитку техніки, технологій, матеріально-технічної та науково-педагогічної бази системи освіти є все можливе для того, щоб в найближчому майбутньому реалізувати цю концепцію і в нашому Східноукраїнському національному університеті ім. В.Даля і скористатися всіма незаперечними перевагами смарт будівлі.

На підставі поставленої мети була запропонована система управління вищим навчальним заклад з використанням технології Інтернету речей, яка дозволить вирішити проблеми енергозбереження та відповідно економити кошти, спрямовані на експлуатацію будівлі.

У розділі «Охорона праці та безпека в надзвичайних ситуаціях» виконано аналіз потенційних небезпек при роботі із засобами обчислювальної техніки і механізмами, розроблені заходи щодо техніки безпеки, заходи, які забезпечують виробничу санітарію і гігієну праці, розраховане штучне освітлення, виконані рекомендації по пожежній безпеці.

Дякую за увагу!