ЕЛЕКТРОНІКА

УДК 004.056.55

Крилов А.В.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Ямненко Ю.С.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

БЕЗПЕКА ІНФОРМАЦІЇ В MICROGRID ІЗ ВПРОВАДЖЕНОЮ КОНЦЕПЦІЄЮ INTERNET OF THINGS

У статті викладено теоретичні принципи побудови системи розподіленої генерації MicroGrid із реалізацією концепції «Інтернету речей» (IoT – Internet of Things). Узгоджене енергоефективне керування електроживленням в MicroGrid набуває особливої актуальності в умовах сучасного розвитку енергетики, електротехніки та електроніки, при великій кількості електротехнічних пристроїв, які суттєво відрізняються за функціональними характеристиками, робочими режимами, рівнем споживання та важливістю для людини. У статті розглянуто два види захисту інформації: використання регульованого фільтру й програмне кодування інформації.

Ключові слова: *MicroGrid, Internet of Things, керований фільтр, алгоритм, мікроконтролер.*

Постановка проблеми. Задача розробки сучасних автоматизованих систем керування та прийняття рішень для систем розподіленої генерації MicroGrid у наш час є досить актуальною [1]. При цьому виникає ряд питань, пов'язаних із безпечною передачею та зберіганням інформації, отриманої з датчиків та контролюючих вузлів системи. Формування єдиного інформаційного середовища, що об'єднує всі наявні в MicroGrid пристрої, є принципово новою умовою формування узгодженого керування в спільному інформаційному середовищі, на відміну від традиційної побудови систем керування електроживленням [2]. Такий підхід забезпечує підвищення рівня «інтелектуалізації» керування електроенергетичними процесами. Тому важливим є залучення новітніх інформаційних методів та технологій для вирішення задачі керування. У цьому напрямку, зокрема, актуальним є підхід до формування єдиного інформаційного середовища за концепцією «Інтернету речей» (IoT – Internet of Things) [3].

Під час впровадження концепції IoT у MicroGrid утворюється локальна інформаційна інфраструктура, здатна до функціонування згідно з встановленими алгоритмами з можливістю доступу та обміну інформацією із зовнішніми об'єктами.

Система MicroGrid

MicroGrid є інноваційною концепцією малої розподіленої енергетики, що передбачає створення локальних мережевих енергетичних структур. Уніфікована структура системи MicroGrid включає акумуляторні батареї, перетворювальні пристрої напруги, контролери заряду/розряду, різнотипні генератори (альтернативні та відновлювальні джерела енергії), а також навантаження (рис. 1). Наявність альтернативних джерел дозволяє забезпечити безперебійність роботи під час відключення централізованої мережі живлення або паралельно з нею. У випадку тривалої відсутності напруги мережі та недостатності енергії від альтернативних джерел відбувається відключення електротехнічних пристроїв з урахуванням їх пріоритетів.

Складові системи

До систем розосередженої генерації MicroGrid відносяться приватні будинки типу SmartHouse,

автономні та/або підключені до центральної електричної мережі локальні електротехнічні об'єкти – дослідницькі станції, фермерські господарства, морські та космічні комплекси. У залежності від типу об'єкту набір датчиків, виконавчих елементів, типів альтернативних джерел може варіюватися.

Необхідними умовами функціонування є виконання всіх технологічних завдань електрообладнання, передбачених специфікою та функціональним призначенням, а також дотримання необхідного рівня комфортності користування та зручності для власника/оператора.

З точки зору керування електроспоживанням застосовуються різні стратегії побудови керуючих алгоритмів, зокрема: централізоване, децентралізоване та комбіноване керування.

Концепція IoT

Результатом впровадження концепції IoT є мережа, що складається з взаємопов'язаних фізичних об'єктів (речей) або пристроїв, які мають вбудовані датчики, виконавчі пристрої, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами за допомогою використання стандартних протоколів зв'язку в дротових або бездротових мережах. Ці взаємопов'язані об'єкти можуть бути запрограмовані на зчитування інформації та приведення в дію пристроїв, що приєднані до них, ідентифікацію користувача, а також дозволяють при потребі виключити участь людини у функціонуванні цих пристроїв за рахунок використання інтелектуальних інтерфейсів [3].

На сьогодні Інтернет речей знаходиться на початковій стадії розвитку. Для його повної реалізації необхідний подальший розвиток існуючих бездротових технологій передачі даних та мережевої інфраструктури, а також покращення існуючої елементної бази пристроїв зчитування інформації та виконання дій (датчиків, вимикачів, тощо). Розвиток Інтернету речей залежить від:

1) технологій бездротових мереж із низьким енергоспоживанням;

2) темпів впровадження стільникових мереж для IoT: EC-GSM, LTE-M, NB – IoT, а також універсальних мереж 5G;

3) переходу мережі Інтернет на версію протоколу IPv6 [4].

Найпоширенішим способом зв'язку в IoT є бездротові мережі, які використовують відповідні технології передавання даних. До цих технологій належать, перш за все, LPWAN (англ. Low-power Wide-area Network – енергоефективна мережа далекого радіусу дії), WLAN (Wireless Local Area Network – бездротова локальна мережа, WPAN (Wireless Private Area Network – бездротова приватна мережа).

На рис. 2 наведено типову технологію бездротової мережі LPWAN.

На рис.1 зображено: кінцеві датчики, представлені сенсорами з вбудованими LPWAN-модулям. Сенсори через бездротовий канал зв'язку з'єднані з LPWAN-станцією, яка охоплює певну зону

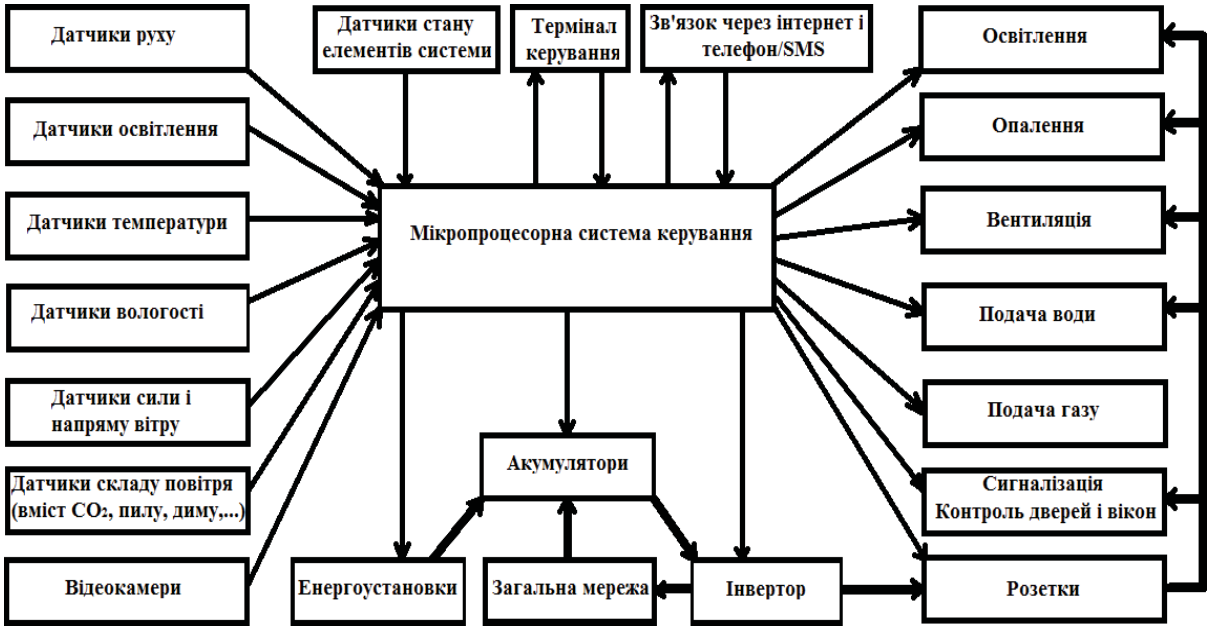

Рис. 1. Приклад структурної схеми MicroGrid – «розумного будинку»

покриття. Разом декілька таких станцій повністю покривають необхідну територію, забезпечуючи безперебійну роботу мережі. У свою чергу, LPWAN-станції з'єднані дротовими каналами зв'язку із сервером, який відіграє роль комутатора. LPWAN використовується для передачі інформації на далекі відстані, а для внутрішнього способу зв'язку використовується менш потужні мережі.

Тож у даній системі є важливим захист інформації. Для забезпечення захисту використовуються два варіанти:

1. **Фізичний метод –** використання регульованих фільтрів джерел живлення мікроконтролера.

2. **Програмний метод** – реалізація програмного кодування інформації.

Розглянемо ці методи більш детально.

Фізичний метод захисту інформації

Ключовим елементом захисту в даному випадку є спеціальним чином сконструйований регульований фільтр на вході живлення мікроконтролера [5]. Система живлення мікроконтролера складається із зовнішнього джерела живлення та фільтру, який живить безпосередньо центральний процесор та пам'ять мікроконтролера та забезпечує спотворення струму живлення для виключення можливості ідентифікації виконуваних команд. Розробка регульованого фільтру живлення є перспективним апаратним методом забезпечення захищеності мікроконтролера від несанкціонованого зчитування за струмом споживання.

Реалізація такої система потребує виконання таких умов:

1) можливість зміни алгоритму захисту без зміни апаратної частини шляхом прошивки мікроконтролера – це необхідно для забезпечення можливості його подальшого вдосконалення;

2) забезпечення відслідковування реального струму споживання мікроконтролера для генерування хибного (спотвореного) струму споживання на основі цих даних.

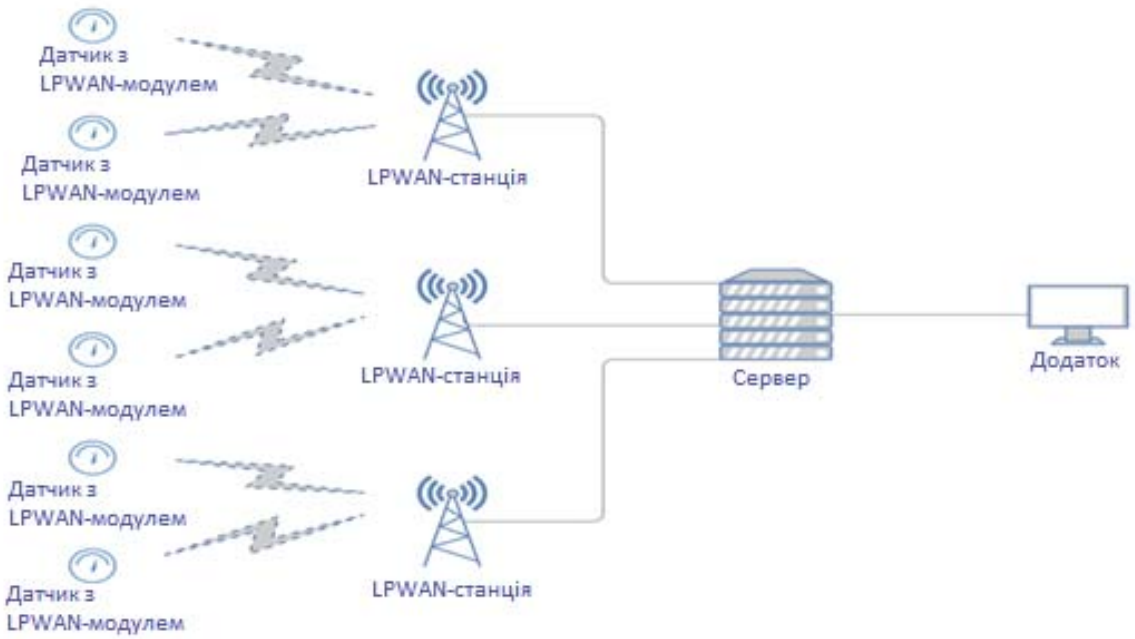

Рис. 2. Типова топологія LPWAN-мережі

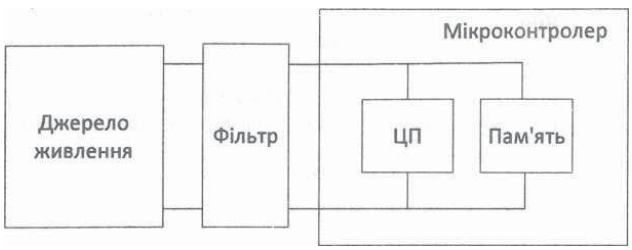

Рис. 3. Структурна схема живлення мікроконтролера з регульованим фільтром захисту

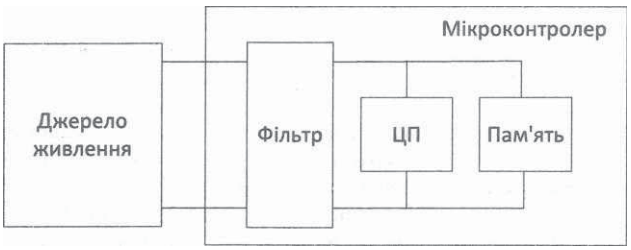

Рис. 4. Перенесення регульованого фільтру живлення у мікроконтролер

Для того щоб отримати інформацію про струм живлення мікроконтролера, потрібно підключитися між фільтром живлення та мікроконтролером. Для підвищення рівня захищеності мікропроцесорної системи від зчитування струму споживання регульований фільтр живлення розміщується всередині корпусу мікроконтролера (рис. 3) або в захищений корпус разом із мікроконтролером (рис. 4).

Параметри фільтру є регульованими і задаються за допомогою системи керування (СК на рис. 5). Вимірювання струму споживання центрального процесора (ЦП) та внутрішньої пам'яті мікроконтролера здійснюється за допомогою датчика струму на активному резисторі та АЦП. Введення додаткового регулювання фільтром дозволяє створити гнучкий алгоритм керування, який змінюється в процесі роботи. Фільтр складається не тільки з ємностей та індуктивностей, як традиційний згладжувальний фільтр, але й містить додаткові активні елементи для генерування шумоподібного сигналу із заданими параметрами, який «домішується» до струму споживання.

На рис. 6 зображено структурну схему пристрою захисту інформації на основі блоку ключів, що складається з кількох комірок, кожна з яких містить ключ на МДН-транзисторі та навантаження.

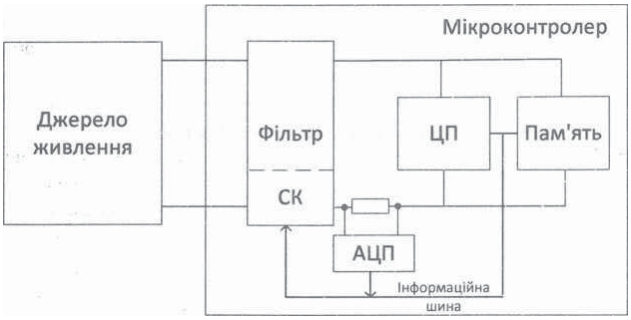

Рис. 5. Фільтр з інформаційною шиною

Завдяки блоку керування генератором випадкових станів досягається внесення додаткових флуктуацій у генеровані випадкові числа, що відповідають станам блоку ключів. Перевагою такої структури фільтру є те, що він не містить конденсаторів великої ємності, а отже, займає меншу площу кристалу.

Введення інформаційної шини дає можливість створювати гнучкі та масштабовані системи електроживлення в сучасних цифрових пристроях на мікропроцесорах. За допомогою інформаційної шини також стає можливим реалізувати алгоритми керування енергоспоживанням у пристроях, що живляться як від акумуляторів, так і від мережі [5].

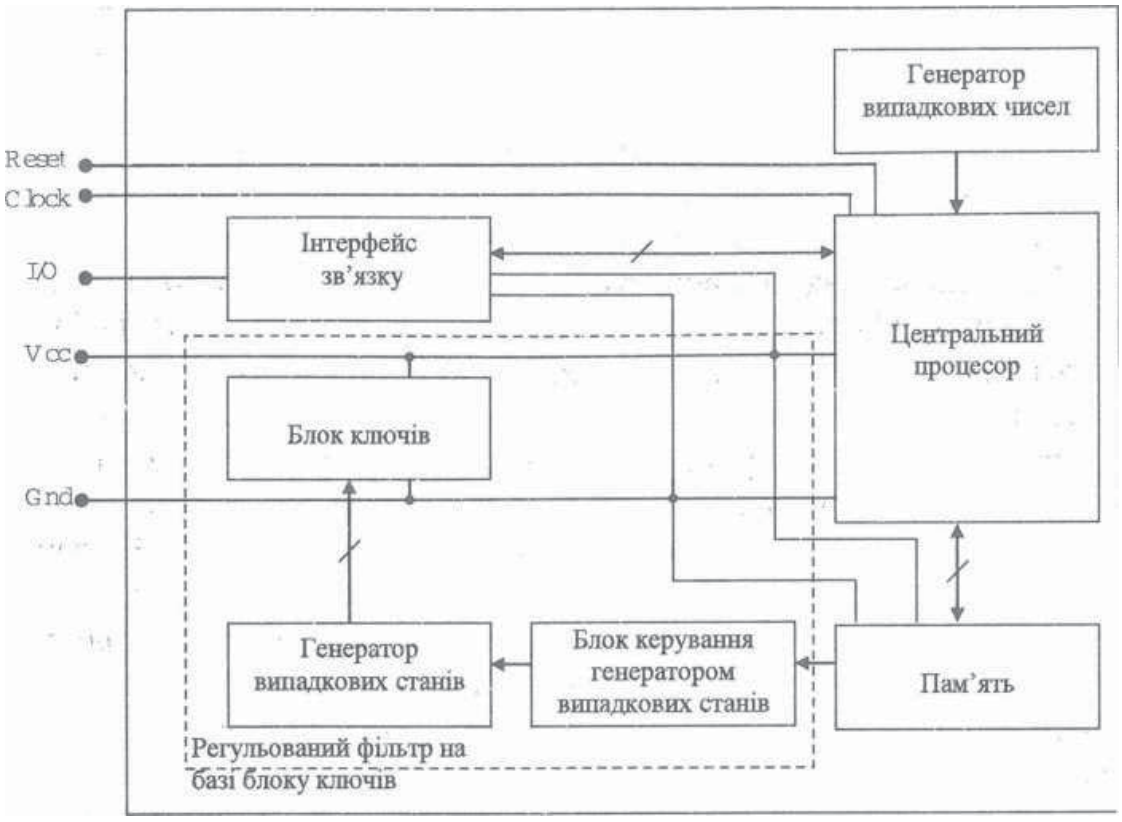

Рис. 6. Структура регульованого фільтра на основі блоку ключів

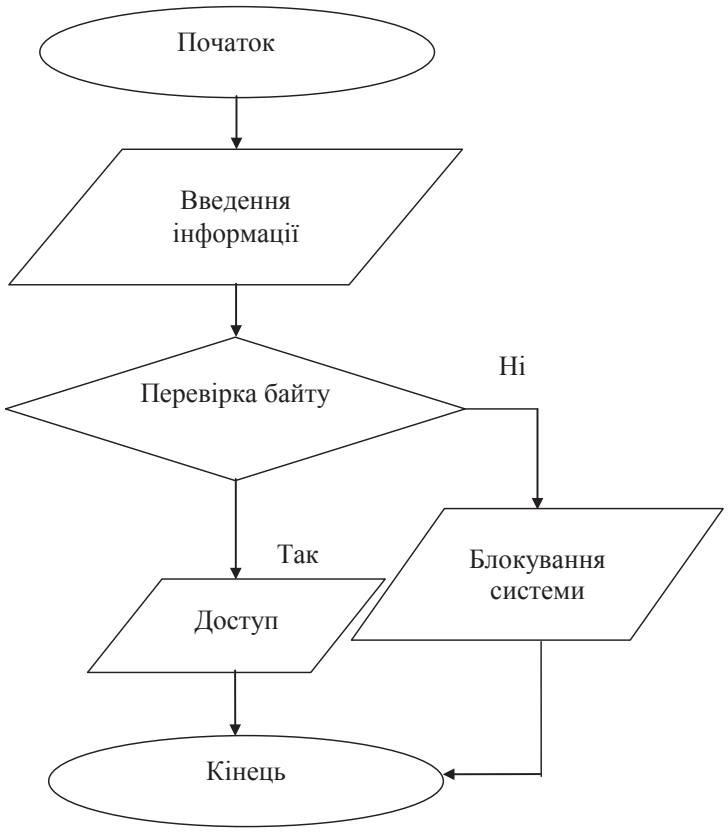

Рис. 7. Алгоритм роботи програмного методу захисту

Програмний метод

Даний метод базується на впровадженні в алгоритм роботи мікроконтролера перевірку початкового допоміжного (перевірочного) байту при передачі коду. У випадку позитивного результату перевірки генерується дозвіл на виконання основної програми, що проілюстровано в алгоритмі на рис. 7.

Під час перевірки задається перевірочний байт, з яким послідовно порівнюються біти початкового байту даних. Для прикладу нижче наведено фрагмент програмного коду при заданому перевірочному байті 10111011 та використанні порту А для передавання інформації по шині даних:

```
void Perevirka(inf) // inf- інформаційне повідомлення з першим перевірочним байтом
{
if(a&1==1 && a&2==0 && a&3==1 && a&4==1 && a&5==1 && a&6==0 && a&7==1 && a&8==1) // перевірка умови
{
A=A;
}
else
A=0;
Порт_Reset=1;
return 0;
}
```

Лістинг частини програми для додавання перевірочного байту В:

```
void_Dod(A)
{
A * pA;
 pA = fopen ("A.txt","r+");// відкриваємо для правки
if (pA!=NULL)// перевірка відкриття
{
fseek(pA, 8, SEEK_SET);//в файлі pA переміщується на 8 позицій вперед відносно початку файлу
fwrite("B", pA);//пишемо туди перевірочний байт B
fclose (pA);
}
```

Також даний метод може бути використаний для організації точки доступу до вузла системи IoT. У цьому випадку ідентифікатор застосовується не для інформаційного повідомлення основної частини коду, а для девайсу з якого здійснюються доступ до бази даних.

Висновки. Реалізація узгодженого керування електротехнічними пристроями в системі розподіленої генерації MicroGrid з реалізацією концепції Інтернету речей дозволяє забезпечити дотримання вимог енергоефективності та інтелектуалізації сучасних електронних систем.

У залежності від функціонального призначення та поставленої задачі керування обмін даними між пристроями загальної системи реалізується з використанням технологій дротового або бездротового зв'язку. Для забезпечення захисту інформації застосовується апаратний метод введення регульованого фільтра джерела живлення мікроконтролера або програмний метод введення додаткового перевірочного байта.

Список літератури:

1. Петергеря Ю.С., Жуйков В.Я. Принципи побудови інтелектуальних систем керування перетворювачів у локальних об'єктах // Зб. праць науково-технічної конференції «Екотехнології і ресурсозбереження. Енергоефективність та охорона навколишнього середовища». К., 2001.
2. Гепко І.А,. Олійник В.Ф., Чайка Ю.Д., Бондаренко А.В. Сучасні бездротові мережі: стан і перспективи розвитку Київ: ЕКМО, 2009., 672 с.
3. Семюел Грінгард «Інтернет речей. Майбутнє вже тут». Видавництво: Альпіна Паблішер, 2016.
4. Росляков А.В., Ваняшин С.В., Гребєшков А.Ю., Самсонов М.Ю. «Інтернет речей» під ред. А.В. Рослякова. Самара: ПГУТІ, ТОВ «Видавництво Ас Гард», 2014. 340 с.
5. Жуйков В.Я, Терещенко Т.О., Ямненко Ю.С., Мороз А.В. Регульовані фільтри джерел живлення для захисту інформації в мікроконтролерах. Видавництво «Кафедра». Київ-2011. С. 43.

БЕЗОПАСНОСТЬ В MICROGRID С ВНЕДРЕННОЙ КОНЦЕПЦИЕЙ INTERNET OF THINGS

В статье изложены теоретические принципы построения системы распределенной генерации MicroGrid с реализацией концепции «Интернета вещей» (IoT – Internet of Things). Согласованное энергоэффективное управления электропитанием в MicroGrid приобретает особую актуальность в условиях современного развития энергетики, электротехники и электроники, при большом количестве электротехнических устройств, которые существенно отличаются по функциональным характеристикам, рабочими режимами, уровню потребления и важности для человека. В статье рассмотрены два вида защиты информации: использование регулируемого фильтра и программное кодирование информации.

Ключевые слова: *MicroGrid, Internet of Things, управляемый фильтр, алгоритм, микроконтролер.*

INFORMATION SECURITY IN MICROGRID WITH THE INTRODUCTION OF THE INTERNET OF THINGS

The article outlines the theoretical principles of constructing a distributed generation MicroGrid system with the implementation of the concept of «Internet of Things» (IoT). Aggregated energy-efficient power management in MicroGrid becomes particularly relevant in today's development of power engineering, electrical engineering and electronics, with a large number of electrical appliances that differ significantly in functionality, operating modes, level of consumption and human importance. Two types of information security are considered in the article – the use of an adjustable filter and programmatic information coding.

Key words: *MicroGrid, Internet of Things, controlled filter, algorithm, microcontroller.*