

УДК 004.056.5: [004.896:728.37]
DOI <https://doi.org/10.26661/2786-6254-2025-2-08>

ІНТЕГРОВАНА СИСТЕМА БЕЗПЕКИ ДЛЯ РОЗУМНОГО БУДИНКУ НА ОСНОВІ GSM-СИГНАЛІЗАЦІЇ

Драєвський Д. С.

викладач

Відокремлений структурний підрозділ «Економіко-правничий фаховий коледж

Запорізького національного університету»

вул. Університетська, 66, Запоріжжя, Україна

orcid.org/0009-0008-3810-6595

draevskdmitry@gmail.com

Мухін В. В.

кандидат технічних наук, доцент,

доцент кафедри програмної інженерії

Запорізький національний університет

вул. Університетська, 66, Запоріжжя, Україна

orcid.org/0009-0007-0270-8239

comentssno@gmail.com

Мильцев О. М.

кандидат фізико-математичних наук,

доцент кафедри програмної інженерії

Запорізький національний університет

вул. Університетська, 66, Запоріжжя, Україна

orcid.org/0009-0009-4382-7730

alexmyltsev@gmail.com

Столярова А. В.

доктор філософії,

доцент кафедри програмної інженерії

Запорізький національний університет

вул. Університетська, 66, Запоріжжя, Україна

orcid.org/0000-0003-2783-2889

stolyarova.a.v@znu.edu.ua

Ключові слова: *інтернет речей, мікроконтролер, GSM-сигналізація, проектування систем, ESP 32.*

З огляду на зростання важливості надійних та автономних систем безпеки в епоху розумних будинків, у цій роботі представлено розроблення та аналіз інтегрованої системи, що використовує GSM-сигналізацію для забезпечення ефективного моніторингу та захисту житлових приміщень. Розглянуто принципи побудови такої системи, зокрема й проектування принципової схеми пристроїв інтернету речей (IoT) для GSM-сигналізації та розроблення відповідного програмного забезпечення. Проаналізовано огляд наявних рішень у сфері безпеки розумних будинків з використанням GSM-технологій, що демонструє їхню ефективність у сповіщенні про загрози та дистанційному реагуванні.

Описано архітектуру розробленої тестової системи, яка включає мікроконтролер NodeMCU ESP32, GSM-модуль SIM800L, датчик руху

PIR, датчик температури та вологості DHT11 та інші компоненти. Представлено алгоритм роботи системи, що підтримує режими охорони та тривоги, керування за допомогою DTMF-команд, сповіщення через SMS та телефонні дзвінки, а також моніторинг наявності мережевої напруги та параметрів навколишнього середовища. Підкреслено актуальність та ефективність інтеграції GSM-сигналізації в системах безпеки розумних будинків, її автономність та можливості розширення завдяки технологіям IoT. Результати дослідження демонструють потенціал розробленої системи для підвищення рівня безпеки житлових приміщень шляхом автоматизованого й оперативного сповіщення користувачів про загрози.

INTEGRATED SECURITY SYSTEM FOR A SMART HOME BASED ON GSM ALARMS

Draevskii D. S.

Lecturer

*Separate Structural Subdivision "Economic and Legal Vocational College
of Zaporizhzhia National University"*

Universytetska str., 66, Zaporizhzhia, Ukraine

orcid.org/0009-0008-3810-6595

draevskdmitry@gmail.com

Mukhin V. V.

Candidate of Technical Sciences, Associate Professor,

Professor at the Software Engineering Department

Zaporizhzhia National University

Universytetska str., 66, Zaporizhzhia, Ukraine

orcid.org/0009-0007-0270-8239

comentssno@gmail.com

Myltsev O. M.

Candidate of Physical and Mathematical Sciences,

Associate Professor at the Software Engineering Department

Zaporizhzhia National University

Universytetska str., 66, Zaporizhzhia, Ukraine

orcid.org/0009-0009-4382-7730

alexmyltsev@gmail.com

Stoliarova A. V.

PhD, Associate Professor at the Department of Software Engineering

Zaporizhzhia National University

Universytetska str., 66, Zaporizhzhia, Ukraine

orcid.org/0000-0003-2783-2889

stolyarova.a.v@znu.edu.ua

Key words: *Internet of Things, microcontroller, GSM alarm, system design, ESP32.*

Given the increasing importance of reliable and autonomous security systems in the era of smart homes, this document presents the development and analysis of an integrated system that uses GSM alarms to ensure effective monitoring and protection of residential premises. The principles of building such a system are examined, including the design of the circuit for Internet of Things (IoT) devices for GSM alarms and the development of the corresponding software. An overview of existing solutions in the field of smart home security using GSM technologies is provided, demonstrating their effectiveness in threat notification and remote response.

The architecture of the developed test system is described, which includes a NodeMCU ESP32 microcontroller, a SIM800L GSM module, a PIR motion sensor, a DHT11 temperature and humidity sensor, and other components. The paper presents the system's operating algorithm, supporting security and alarm modes, control via DTMF commands, notifications through SMS and phone calls, as well as monitoring of the availability of network voltage and environmental parameters.

Particular emphasis is placed on the relevance and effectiveness of integrating GSM alarms into smart home security systems, highlighting their autonomy and potential for expansion through IoT technologies. The research results demonstrate the potential of the developed system to enhance the security level of residential premises by providing automated and prompt notification of threats to users.

Вступ. У сучасному світі питання гарантування безпеки житлових приміщень набуває все більшого значення. Зростання кількості розумних будинків і розвиток технологій автоматизації сприяють впровадженню інноваційних методів контролю та захисту. Одним із найефективніших рішень для убезпечення є інтеграція GSM-сигналізації в систему охорони розумного будинку. Дана технологія дозволяє здійснювати моніторинг у реальному часі, передавати сповіщення про загрози, виконувати автоматичні дзвінки на мобільні пристрої власників і забезпечувати оперативне реагування на надзвичайні ситуації [1].

Використання GSM-зв'язку в системах безпеки дає можливість створювати автономні рішення, які не залежать від дротового інтернет-з'єднання або локальних мереж. Окрім того, інтеграція GSM із технологіями інтернету речей (далі – IoT) відкриває нові можливості для підвищення ефективності та надійності систем захисту житла [2]. Останні дослідження демонструють, що GSM-сигналізація в поєднанні з розумними датчиками руху й автоматичними дзвінками власникам дозволяє суттєво покращити рівень безпеки житлових приміщень [3].

Об'єктом дослідження є інтегрована система безпеки для розумного будинку, що використовує GSM-сигналізацію для передавання повідомлень, виконання дзвінків і моніторингу стану безпеки.

Метою дослідження є аналіз і розроблення інтегрованої системи безпеки для розумного будинку на основі GSM-сигналізації, яка дозволяє забезпечити ефективний моніторинг і захист житлового приміщення шляхом автоматизованого сповіщення користувачів про загрози через повідомлення та телефонні дзвінки.

Для досягнення поставленої мети необхідно виконати такі завдання: спроектувати принципову схему пристроїв IoT для GSM-сигналізації; розробити програмну реалізацію GSM-сигналізації. **Огляд літератури.** Огляд літератури охоплює низку досліджень та розробок у галузі безпеки розумних будинків, зокрема через застосування GSM-сигналізації, що дозволяє забезпечити ефективний моніторинг і контроль за станом безпеки на відстані.

У статті [4] представлено автоматизовану систему виявлення вторгнень для будинків і офі-

сів, яка поєднує різні сенсори, як-от PIR-датчики та магнітні перемикачі, із GSM-модулем для сповіщення власників про несанкціонований доступ через телефонні дзвінки.

У роботі [5] запропоновано систему безпеки для розумного будинку, яка використовує GSM для надсилання SMS власникам у разі виявлення аномалій сенсорами. Система також включає механізм автентифікації для забезпечення доступу лише авторизованих користувачів і мережеву систему виявлення вторгнень для сповіщення про підозрілу активність у мережі IoT.

У [6] розглянуто концепцію «розумного дому» – автоматизованої системи для керування побутовими електричними пристроями. Основна мета – підвищення комфорту, безпеки та зручності для мешканців. Система дозволяє автоматично керувати навантаженнями (приладами), виявляти пожежу, контролювати температуру, розпізнавати рух, управляти замками дверей. Окрім того, система має розширені функції безпеки: у разі підозрілої події в оселі надсилає повідомлення користувачу. Також передбачено дистанційне керування приладами через мобільний телефон з використанням технології GSM. Загалом, робота демонструє, як автоматизація побуту може значно покращити якість життя, підвищити безпеку та дати змогу користувачеві контролювати дім навіть на відстані.

Актуальність систем домашньої безпеки в умовах зростання загроз, як-от вторгнення, витік газу чи пожежа, розглядається у статті [7]. Традиційні сигналізації обмежуються лише звуковим попередженням, тоді як GSM-технології дозволяють значно розширити можливості безпеки. Запропоновано дві системи захисту: систему з вебкамерою – реагує на рух, видає звуковий сигнал і надсилає власнику електронного листа, систему на базі GSM-GPS-модуля (SIM548с) з мікроконтролером Atmega644p – у разі спрацювання датчиків надсилає SMS власнику, активує реле та звуковий сигнал.

Отже, робота демонструє ефективне використання сучасних технологій для оперативного сповіщення та дистанційного реагування на загрози в будинку.

Систему керування домашніми приладами (світло, вентилятор, холодильник та інші) та вияв-

лення підозрілої активності, зокрема крадіжок, за допомогою PIR-датчика руху представлено в роботі [8]. Ключові особливості: у разі виявлення руху в домі за відсутності власника PIR-датчик активує камеру, яка робить знімок і надсилає його користувачу через Raspberry Pi; водночас через GSM-модуль надсилається SMS; мікроконтролер PIC16F877A дозволяє дистанційно вмикати/вимикати прилади через мобільний телефон, що допомагає економити електроенергію; у разі пожежі спеціальний датчик передає сигнал користувачу, якщо температура перевищує норму.

Система відзначається низьким енергоспоживанням, швидкою обробкою сигналів, надійністю та зручністю доступу з будь-якої точки через GSM-зв'язок.

Розроблення системи безпеки для дому, яка забезпечує автоматичне сповіщення власника та відповідних служб (поліції, пожежної та інших) у разі спроби несанкціонованого проникнення, розглядається в роботі [9].

Основна ідея – створити систему, яка працює автономно, без потреби постійного контролю з боку користувача. У разі небезпеки контролер активує GSM-модуль, що надсилає SMS-повідомлення власнику та службам реагування.

Отже, система дозволяє поєднати домашню автоматизацію з ефективним захистом, водночас залишається доступною за ціною.

Стаття [10] присвячена системі автоматизації дому на базі Arduino Mega2560, яка поєднує керування приладами з функціями безпеки. Система дозволяє автоматично керувати домашніми пристроями, а також забезпечує захист від вторгнень, пожежі, витоку газу та CO. Використовує такі компоненти: датчики (руху, диму, газу), GSM-модуль для надсилання SMS у разі небезпеки, реле для керування приладами, звукові сигнали (бузери), мобільний застосунок для дистанційного керування.

Система забезпечує доступність, надійність і зручність, демонструє переваги сучасних мікропроцесорних технологій для створення розумного будинку за низькою вартістю.

Робота [11] представляє бездротову систему безпеки для дому на основі GSM-модуля, яка вирізняється низьким енергоспоживанням і швидкою реакцією на вторгнення. Основні елементи: магнітний датчик з реле на дверях, що фіксує спробу входу, GSM-модем, який миттєво надсилає SMS або здійснює дзвінок власнику в разі виявлення загрози.

Система дозволяє контролювати безпеку дому з будь-якого місця через мобільну мережу й інформує власника про підозрілу активність заздалегідь запрограмованим повідомленням.

Проведений огляд літератури демонструє значний інтерес і активне розроблення систем

домашньої безпеки на основі GSM-технологій. Наявні рішення варіюються від простих систем сповіщення про вторгнення до комплексних платформ керування розумним будинком з розширеними функціями безпеки, як-от виявлення пожежі чи витоку газу та дистанційне керування приладами. Спільними рисами багатьох розробок є використання GSM-модулів для оперативного сповіщення власників про небезпеку через SMS або телефонні дзвінки, а також прагнення до автономності, низького енергоспоживання та зручного дистанційного керування.

Однак, незважаючи на значну кількість існуючих рішень, огляд літератури також виявляє потенційні напрями для вдосконалення та актуальність розроблення власної GSM-сигналізації. Аналіз показав, що існуючі системи часто є спеціалізованими або мають обмежену гнучкість у налаштуванні й інтеграції.

Розроблення доступної за ціною GSM-сигналізації з функцією постійного моніторингу температури зумовлене низькою важливих соціально-економічних і практичних факторів, особливо в умовах нестабільної економічної ситуації.

Функція постійного моніторингу температури в поєднанні із GSM-сповіщеннями надає власникам можливість дистанційно відстежувати температурний режим у своїх оселях. Це особливо актуально в разі тривалої відсутності (відраджень, відпустки, сезонне проживання на дачі). Отримання своєчасного сповіщення про критичне зниження температури дозволяє оперативно вжити заходів для запобігання серйозним наслідкам, наприклад, попросити сусідів перевірити стан опалення або дистанційно перезапустити систему, якщо це можливо.

Завчасне виявлення проблем з опаленням завдяки моніторингу температури може допомогти уникнути значних фінансових втрат, пов'язаних з ремонтом або заміною пошкодженого обладнання та ліквідацією наслідків замерзання систем водопостачання та опалення.

Методи. Архітектурні особливості IoT-пристроїв і відповідного програмного забезпечення розглянуто на прикладі системи GSM-сигналізації. Для створення тестового проєкту використовувалися широкодоступні IoT-пристрої, що не потребують спеціальних налаштувань.

До складу системи входять такі компоненти: мікроконтролер NodeMCU ESP32 – центральний керівний модуль, який отримує сигнали від датчиків і надсилає команди іншим пристроям; детектор напруги з оптопарою – контролює наявність змінного струму 220 В та передає відповідний сигнал мікроконтролеру; модуль SIM800L – забезпечує зв'язок із GSM-мережею, виконує надсилання SMS, приймає вхідні дзвінки та здійснює

виклики; DFPlayer Mini – використовується для відтворення заздалегідь записаних голосових повідомлень; датчик руху PIR – виявляє рух у контрольованій зоні й активує тривожний сигнал; датчик температури та вологості DHT11 – фіксує параметри навколишнього середовища, які можуть бути включені до системного звіту; світлодіод із резистором – забезпечує візуальну індикацію стану системи: увімкнена охорона, активована тривога або система вимкнена.

Рисунок 1 відображає електричну схему пристроїв, які використовуються для системи GSM-сигналізації.

Для демонстрації програмної реалізації GSM-сигналізації розглянемо ключові етапи розроблення програмного забезпечення для мікроконтролера, який керуватиме GSM-модулем і датчиками.

Програмна реалізація GSM-сигналізації передбачає розроблення таких основних модулів:

1. Ініціалізація обладнання (setup()). Цей модуль відповідає за початкове налаштування всіх апаратних компонентів системи, включаючи послідовні порти, GSM-модуль, аудіоплеєр, датчики та піни введення – виведення:

```
void setup() { Serial.begin(115200); // Налаштування SIM800L
```

```
sim800.begin(9600, SERIAL_8N1, SIM800_RX, SIM800_TX);
```

```
sendATCommand("AT");
sendATCommand("AT+CLIP=1"); // Відображення номера вхідного дзвінка
sendATCommand("AT+CMGF=1"); // Текстовий режим SMS
sendATCommand("AT+DDEET=1"); // Увімкнути детекцію DTMF
Serial.println("SIM800L готовий");
// Налаштування DFPlayer Mini
dfPlayerSerial.begin(9600, SERIAL_8N1, DFPLAYER_RX, DFPLAYER_TX);
if (!dfPlayer.begin(dfPlayerSerial)) { Serial.println("Помилка ініціалізації DFPlayer Mini!");
while (true); }
dfPlayer.volume(30); Serial.println("DFPlayer Mini готовий."); pinMode(PIR_PIN, INPUT);
pinMode(VOLTAGE_PIN, INPUT_PULLUP); pinMode(LED_PIN, OUTPUT); dht.begin();
updateLED(); // Відобразити початковий стан
Serial.println("Система сигналізації готова."); }
```

2. Обробка вхідних дзвінків (handleIncomingCall()). Цей модуль відповідає за прослуховування вхідних дзвінків, ідентифікацію номера абонента й обробку DTMF-команд, що надходять під час розмови.

```
void handleIncomingCall() {
if (sim800.available()) { String response = sim800.readString();
```

```
Serial.println("Відповідь SIM800L: " + response);
```

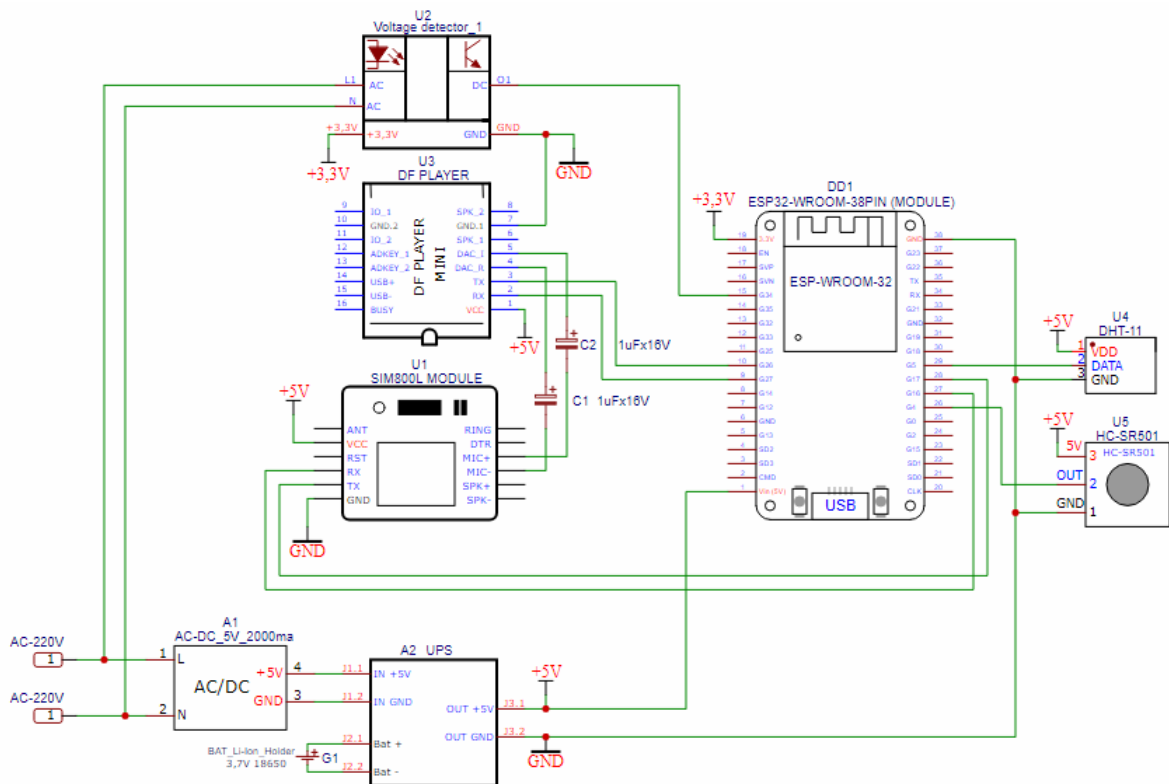


Рис. 1. Електрична схема GSM сигналізації

```

if (response.indexOf("+CLIP:") != -1) { String
caller = extractNumber(response);
if (isNumberAllowed(caller)) { answerCall();
delay(1000); playVoiceMenu();
} else { rejectCall(); }}
// Обробка DTMF-входів
if (response.indexOf("+DTMF:") != -1) {
char dtmf = response.charAt(response.
indexOf("+DTMF:") + 7);
processDTMFCommand(dtmf); }}

```

3. Керування голосовими повідомленнями (playVoiceMenu(), playVoiceMessage()). Цей модуль відповідає за відтворення попередньо записаних голосових повідомлень через аудіоплеєр DFPlayer Mini для інформування користувача про стан системи або для голосового меню керування.

```

// Відтворити голосове меню
void playVoiceMenu() {
if (isAlarmTriggered) { playVoiceMessage(1); //
Тривога
} else if (isArmed) { playVoiceMessage(2); //
Охорона ввімкнена
} else { playVoiceMessage(3); // Охорона
вимкнена
}}

```

// Відтворення голосового повідомлення через DFPlayer

```

void playVoiceMessage(int fileNumber) {
dfPlayer.play(fileNumber); delay(6000); }

```

4. Обробка DTMF-команд (processDTMFCommand()). Цей модуль інтерпретує натискання кнопок на телефоні (DTMF-сигнали) під час вхідного дзвінка та виконує відповідні дії, як-от зміна стану охорони, скидання тривоги або отримання звіту.

```

// Обробка DTMF-команд
void processDTMFCommand(char dtmf) {
Serial.println("Отримано DTMF: " +
String(dtmf));
switch (dtmf) { case '0': playVoiceMenu(); break;
case '1': if (isAlarmTriggered) { isAlarmTriggered
= false; updateLED();
playVoiceMessage(4); // Тривогу зупинено
} break;
case '2': isArmed = true; updateLED();
playVoiceMessage(2); // Охорона ввімкнена
break;
case '3': isArmed = false; updateLED();
playVoiceMessage(3); // Охорона вимкнена
break;
case '6': sendSystemReport(); break; default:
Serial.println("Невідома команда.");
break; }}

```

5. Надсилання SMS-повідомлень (sendSMS()). Цей модуль відповідає за формування та відправку SMS користувачам у разі три-

воги, зміни стану напруги або за запитом звіту про стан системи.

```

// Відправка SMS
void sendSMS(const String& message) {
sendATCommand("AT+CMGS=\
"+380999623204\"); delay(200);
sim800.println(message); sim800.write(26);
delay(2000); }

```

6. Керування GSM-модулем (sendATCommand()). Цей модуль забезпечує низькорівневу комунікацію із GSM-модулем SIM800L шляхом відправки AT-команд і отримання відповідей.

```

// Відправка AT-команди з логами
void sendATCommand(const char* command) {
sim800.println(command); delay(1000);
while (sim800.available()) { char c = sim800.
read(); Serial.print(c); }
Serial.println(); }

```

7. Перевірка дозволених номерів (isNumberAllowed()). Цей модуль відповідає за авторизацію вхідних дзвінків шляхом порівняння номера абонента зі списком попередньо визначених дозволених номерів.

```

// Перевірка, чи номер дозволений
bool isNumberAllowed(const String& number) {
for (int i = 0; i < 2; i++) { if (number.
indexOf(allowedNumbers[i]) != -1) {
return true; }} return false; }

```

8. Визначення номера абонента (extractNumber()). Цей модуль вилучає номер телефону з текстової відповіді GSM-модуля на вхідний дзвінок.

```

// Витягнення номера із вхідного дзвінка
String extractNumber(const String& response) {
int startIndex = response.indexOf("\"") + 1;
int endIndex = response.indexOf("\",", startIndex);
return response.substring(startIndex, endIndex); }

```

9. Візуалізація стану системи (updateLED()). Цей модуль відповідає за відображення поточного стану системи (охорона ввімкнена, тривога) за допомогою світлодіода.

```

// Оновлення стану світлодіода
void updateLED() { if (isAlarmTriggered) { for
(int i = 0; i < 10; i++) {
digitalWrite(LED_PIN, HIGH); delay(200);
digitalWrite(LED_PIN, LOW);
delay(200); }} else if (isArmed) {
digitalWrite(LED_PIN, HIGH); } else {
digitalWrite(LED_PIN, LOW); }}

```

10. Моніторинг датчика руху (checkPIR()). Цей модуль періодично перевіряє стан датчика руху й ініціює режим тривоги в разі виявлення руху, коли система перебуває під охороною.

```

// Перевірка руху
void checkPIR() {
if (isArmed && digitalRead(PIR_PIN) == HIGH)
{ isAlarmTriggered = true;
activateAlarm(); }}

```

11. Контроль напруги живлення (checkVoltage()). Цей модуль періодично перевіряє наявність напруги 220В та надсилає відповідне текстове повідомлення в разі її зникнення або відновлення.

```
// Перевірка напруги
void checkVoltage() {
    bool currentVoltageState =
digitalRead(VOLTAGE_PIN) == LOW;
    if (currentVoltageState != voltagePresent) {
        voltagePresent = currentVoltageState;
        sendSMS(voltagePresent ? "Voltage: 220 V is
available." : "Voltage: 220 V no.");} }
```

12. Активація режиму тривоги (activateAlarm()). Цей модуль виконує дії в разі тривоги, як-от надсилання SMS і запуск процедури обдзвонювання дозволених номерів.

```
// Активація тривоги
void activateAlarm() {
    sendSMS("The alarm is triggered!");
    callPhone(allowedNumbers[currentNumberIn
dex]); lastCallTime = millis();
    updateLED(); }
```

13. Здійснення голосових викликів (callPhone()). Цей модуль відповідає за ініціювання голосових викликів на дозволени номери в разі тривоги, з можливістю повторних спроб.

```
// Виклик номера в разі тривоги
void callPhone(const char* phoneNumber) {
    sendATCommand(("ATD" + String(phoneNumber)
+ ";" ).c_str()); delay(20000); // Очікування підняття
трубки
    // Якщо трубку не підняли, спробувати наступ-
ний номер або повторити через 10 хвилин
    if (millis() - lastCallTime > 600000) { // 10 хвилин
        currentNumberIndex = (currentNumberIndex +
1)% 2; // Переходимо до наступного номера
        lastCallTime = millis();
        if (currentNumberIndex == 0) {// Якщо всі
номери обдзвонені, повторити через 10 хвилин
            callPhone(allowedNumbers[currentNumberIn
dex]); } } }
```

14. Формування звіту про стан системи (sendSystemReport()). Цей модуль збирає інформацію про температуру, вологість та стан напруги живлення та надсилає її користувачеві SMS за запитом.

```
// Відправка звіту
void sendSystemReport() {
    float temperature = dht.readTemperature(); float
humidity = dht.readHumidity();
    String voltage = voltagePresent ? "220 V is
available" : "There is no 220 V";
    String report = "Temperature: " +
String(temperature, 1) + "C, Humidity: " +
String(humidity, 1) + "%, High-voltage: " + voltage;
    sendSMS(report); }
```

Ці етапи відображають основні функціональні блоки та логіку роботи розробленої GSM-сигналізації на базі мікроконтролера. Кожен етап відповідає за визначену частину функціональності системи, починаючи від ініціалізації обладнання і закінчуючи обробкою тривожних подій і взаємодією з користувачем.

Такий підхід дозволяє створити надійну й адаптивну систему безпеки, що реагує на різні сценарії та забезпечує безперебійне функціонування.

Результати. Розглянемо алгоритм і логіку управління охороною тестового проєкту, де система може функціонувати у двох режимах: «Охорона активована» або «Охорона деактивована», причому зміна між цими режимами відбувається шляхом уведення DTMF-команд – натискання '2' активує охорону, а '3' її вимикає.

Коли система перебуває в режимі «Охорона активована», а пасивний інфрачервоний датчик (PIR) виявляє рух, спрацьовує сигнал тривоги. У цьому стані система автоматично відправляє текстове повідомлення, здійснює телефонний виклик та активує світлову індикацію (блимання LED, сирена). Для скасування тривоги та повернення об'єкта під охорону використовується DTMF-команда '1'.

Усі вхідні дзвінки проходять перевірку на відповідність списку авторизованих номерів (максимум чотири).

У процесі виконання проєкту за допомогою Android-застосунку T2S: Text to Voice/Read Aloud було згенеровано три аудіофайли – 0001.mp3, 0002.mp3 і 0003.mp3. Далі ми детально розглянемо, як саме структуровано інформацію в кожному із цих файлів.

Файл 0001.mp3. Охорону вимкнено. Увімкнути охорону – натисніть 2. Сформувати системний звіт – натисніть 6. Прослухати ще раз – натисніть 0.

Файл 0002.mp3. Охорона ввімкнена. Вимкнути охорону – натисніть 3. Сформувати системний звіт – натисніть 6. Прослухати ще раз – натисніть 0.

Файл 0003.mp3. Тривога в зоні 1. Тривога ввімкнена. Вимкнути тривогу – натисніть 1. Охорона ввімкнена. Вимкнути охорону – натисніть 3. Сформувати системний звіт – натисніть 6. Прослухати інформацію ще раз – натисніть 0.

Щоб файли стали доступними для системи, їх треба перенести на SD-карту за допомогою пристрою для читання карт пам'яті. Для безперебійного відтворення модулем DFPlayer Mini файли повинні мати точні імена (0001.mp3, 0002.mp3, 0003.mp3) і розташовуватися в головному каталозі SD-карти.

Модуль DFPlayer Mini забезпечує відтворення потрібних аудіозаписів із SD-карти у відповідь на команди системи. Наприклад, залежно від поточного стану сигналізації (активована, деактивована).

вана, тривога) або отриманих DTMF-сигналів, будуть програватися відповідні звукові файли.

Завдяки технології DTMF користувач має можливість:

- дізнатися поточний стан системи (натиснувши ‘0’);
- вимкнути режим тривоги (натиснувши ‘1’);
- перемикає режим охорони (активувати за допомогою ‘2’, деактивувати – ‘3’);
- запросити звіт про поточний стан системи (натиснувши ‘6’).

Система здійснює постійний нагляд за наявністю електроживлення 220 В. Також відбувається моніторинг температури та рівня вологості повітря за допомогою датчика DHT11.

Продовжимо опис функціональності тестового проєкту, далі буде представлено детальний алгоритм роботи системи охоронної сигналізації, а також відповідна блок-схема (рис. 2), що візуалізує логіку її функціонування.

1. Початок.

2. Перевірка вхідного дзвінка:

- якщо є вхідний дзвінок, перейти до кроку 3;
- якщо немає вхідного дзвінка, повернутися до кроку 2 (очікування дзвінка).

3. Перевірка номера:

- якщо номер вхідного дзвінка є у списку дозволених, перейти до кроку 4;
- якщо номер відсутній у списку дозволених, відхилити дзвінок і повернутися до кроку 2.

4. Перевірка напруги 220 В:

- якщо напруга 220 В відсутня, перейти до кроку 5;
- якщо напруга 220 В присутня, перейти до кроку 8.

5. Перехід на автономне живлення.

6. Постійна перевірка напруги 220 В:

- якщо напруга 220 В з’явилася, перейти до кроку 7;
- якщо напруга 220 В відсутня, повернутися до кроку 6.

7. Перехід на живлення 220 В.

8. Очікування DTMF-команди:

- якщо отримана команда ‘0’, повідомити поточний стан системи та повернутися до кроку 8;
- якщо отримана команда ‘2’, активувати режим охорони та перейти до кроку 9;
- якщо отримана команда ‘3’, деактивувати режим охорони та повернутися до кроку 8;
- Якщо отримана команда ‘6’, надати розширений звіт про стан системи та повернутися до кроку 8.

9. Контроль датчика руху:

- якщо зафіксовано рух, перейти до кроку 10;
- якщо руху немає, залишатися на кроці 9 (продовжувати контроль).

10. Увімкнення сирени та надсилання SMS.

11. Здійснення дзвінка на дозволені номери по черзі.

12. Очікування відповіді на дзвінок:

- якщо на дзвінок відповіли, перейти до кроку 13;
- якщо на дзвінок не відповіли всі дозволені номери, повернутися до кроку 11 (повторний дзвінок).

13. Очікування DTMF-команди після дзвінка:

- якщо отримана команда ‘1’, деактивувати сирену та повернутися до кроку 9 (система залишається в режимі охорони);
- якщо отримана команда ‘3’, деактивувати режим охорони та повернутися до кроку 8;
- якщо отримана інша команда, повернутися до кроку 13 (очікування команди).

14. Контроль живлення 220 В (під час роботи від мережі):

- якщо напруга 220 В зникла, перейти до кроку 5 (перехід на автономне живлення).

15. Постійна перевірка напруги 220 В (під час роботи від автономного живлення):

- якщо напруга 220 В з’явилася, перейти до кроку 7 (перехід на живлення 220 В);
- після переходу на автономне живлення (крок 5) система також переходить до кроку 8 (очікування DTMF-команд).

Розглянутий алгоритм детально описує логіку роботи розробленої GSM-сигналізації, зокрема: керування режимами охорони, обробку тривожних подій з оповіщенням, дистанційне керування за допомогою DTMF-команд, голосові підказки та контроль зовнішніх умов живлення, що забезпечує комплексний підхід до безпеки об’єкта.

Висновки. У сучасних умовах питання забезпечення житлових приміщень є надзвичайно актуальним, розвиток технологій автоматизації та розумних будинків сприяє впровадженню новітніх методів контролю та захисту. Упровадження GSM-сигналізації в системи охорони розумного будинку стає одним з найефективніших рішень для досягнення безпеки, оскільки дозволяє здійснювати моніторинг у реальному часі й оперативно сповіщати власників про потенційні загрози.

Використання GSM-зв’язку дозволяє створювати автономні рішення, незалежні від дротових інтернет-з’єднань або локальних мереж, що підвищує мобільність і надійність систем безпеки. Водночас інтеграція GSM з технологіями інтернету речей (IoT) відкриває нові можливості для підвищення ефективності та надійності охоронних систем.

Дослідження показують, що поєднання GSM-сигналізації з розумними датчиками руху й автоматичними дзвінками власникам значно покращує рівень безпеки житлових приміщень, що робить ці системи більш ефективними в боротьбі із крадіжками й іншими загрозами.

JITEPATYPA

1. Manjushree N., Ashish K. D. GSM and Arduino based Smart Home Safety and Security System. *Recent Trends in Information Technology and its Application*. 2023. Vol. 6. № 1. P. 1–6. DOI: 10.5281/zenodo.7610756
2. Rana G. M. Sultan M., Khan Abdullah Al Mamun, Hoque Mohammad Nazmul, Mitul Abu Farzan. Design and implementation of a GSM based remote home security and appliance control system. *2013 International Conference on Advances in Electrical Engineering (ICAEE)*, Dkaka, Bangladesh, 19–21 December 2013. 2013. DOI: 10.1109/icaee.2013.6750350
3. Oyekola P., Oyewo T., Oyekola A., Mohamed A. Arduino Based Smart Home Security System. *International Journal of Innovative Technology and Exploring Engineering*. 2019. Vol. 8. № 12. P. 2880–2884. DOI: 10.35940/ijitee.l3052.1081219
4. Arinde V. Adeshina, Idowu L. Multi-sensor Intrusion Detection System. arXiv preprint. 2023. URL: <https://arxiv.org/pdf/2406.05137>
5. Hadi H. J., Nisa K. U., Harris S. Autonomous and Collaborative Smart Home Security System (ACSHSS). *arXiv preprint*. 2023. URL: <https://arxiv.org/abs/2309.02899>
6. Mustafijur Rahman, Zaidul Karim A. H. M., Sultanur Nyeem, Faisal Khan, Golam Matin. Microcontroller Based Home Security and Load Controlling Using Gsm Technology. *International Journal of Computer Network and Information Security*. 2015. Vol. 7. № 4. P. 29–36. DOI: 10.5815/ijenis.2015.04.04
7. Bangali J., Shaligram A. Design and Implementation of Security Systems for Smart Home based on GSM technology. *International Journal of Smart Home*. 2013. Vol. 7. № 6. P. 201–208. DOI: 10.14257/ijsh.2013.7.6.19
8. Shetty N. P. Design of Smart Home Security Surveillance System Using GSM. *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering*. 2016. Vol. 4. № 2. P. 54–59. DOI: 10.17148/ijireeice/ncaee.2016.11
9. Sadeque Reza Khan, Ahmed Al Mansur, Alvir Kabir, Shahid Jaman, Nahian Chowdhury. Design and Implementation of Low Cost Home Security System using GSM Network. *International Journal of Scientific & Engineering*. 2012.
10. Motaz Daadoo, Shadi M.A Atallah, Saed Tarapiah. Development of Low Cost Safety Home Automation System using GSM Network. *European Journal of Social Sciences*. 2016. Vol. 53. № 3. P. 338–353.
11. Abhishek S. Parab, Amol Joglekar. Implementation of Home Security System using GSM module and Microcontroller. *International Journal of Computer Science and Information Technologies*. 2015. Vol. 6 (3). P. 2950–2953.

Дата першого надходження рукопису до видання: 25.08.2025
 Дата прийнятого до друку рукопису після рецензування: 22.09.2025
 Дата публікації: 31.12.2025