ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ТА ЕЛЕКТРОННА ІНЖЕНЕРІЯ
INFORMATION AND COMMUNICATION TECHNOLOGIES, ELECTRONIC ENGINEERING

№ 1 (1), 2021

РОЗРОБКА БЕЗПРОВІДНОЇ СИСТЕМИ ЗАВАДОСТІЙКОЇ СИГНАЛІЗАЦІЇ НА БАЗІ ТЕХНОЛОГІЇ LORA

С. Фабіровський, О. Москалюк
Національний університет "Львівська політехніка", вул. С. Бандери, 12, Львів, 79013, Україна

Відповідальний за рукопис: Сергій Фабіровський (e-mail: serhii.y.fabirovskyi@lpnu.ua).

(Подано 16 червня 2021)

Стаття стосується розроблення безпровідної системи завадостійкої сигналізації зі зворотним зв'язком на базі технології LoRa. Актуальність роботи полягає у тому, що питання захисту свого майна від грабіжників завжди важливе. Також важливо, щоб система сигналізаці була універсальною і недорогою річчю, яка окупиться за короткий проміжок часу, водночас забезпечувала б високий рівень захисту. Сьогодні проблема у тому, що навіть за просту систему захисту доведеться добре заплатити, не тільки за сам пристрій, але й за його інсталяцію. Під час інсталяції прилад під'єднують до бортової системи автомобіля, і ця операція також коштує немало. У майбутньому, якщо система зламається, доведеться везти автомобіль в сервіс і деінсталювати, а в машині залишаться порізані проводи. Усе це спонукає до розроблення схожої системи, яка не матиме таких недоліків, яку зможе купити кожен й інсталяція якої не потребуватиме професійних навичок. Саме це стало основною ідеєю цієї роботи.

Ключові слова: *LoRa; сигналізація; STM32; кодування; шифрування.*
УДК: 654.93, 654.16

1. Вступ

Сьогодні дуже популярними стали різноманітні системи сигналізації [1–3], що використовують для захисту як нерухомості, так і транспортних засобів. Таку популярність вони здобули через різноманітні крадіжки, які не припиняються і нині. Найкриміногеннішими серед цих випадків є крадіжки транспортних засобів.

Устаткування охоронної сигналізації є найефективнішим засобом захисту від несанкціонованого проникнення, оскільки видає сигнал тривоги із зазначенням місця порушення задовго до того, як зловмиснику вдасться скоїти злочин.

Основну роль під час створення систем сигналізації відіграють сигнальні сповіщувачі, ще їх називають сенсорами. Від якості їх роботи залежить ефективне функціонування усієї системи загалом. До них ставлять певні вимоги щодо чутливості. На практиці помилкове спрацювання спричиняє матеріальні затрати.

Інтелектуальні багатоканальні системи сигналізації сьогодні добре справляються із таким завданням. Їх ще називають мультисенсорними. До їх складу входять різні сенсори виявлення порушника, але схема обробки інформації в них одна, тобто вони працюють за одним розробленим алгоритмом. Сповіщувачі, що реагують на два або більше чинників, ефективніші й допомагають з більшою імовірністю виявити порушника, порівняно із тими, що реагують тільки на один чинник. Такі системи дають змогу істотно знизити вірогідність помилкового спрацювання сигналізації.

Також дуже важливу роль відіграють дальність зв'язку і його завадозахищеність, яку можна реалізувати, задіявши сучасні технології, такі як LoRa [4, 5]. Поєднавши доступні новітні технології, можна досягти високої енергоефективності, дальності зв'язку й отримати нові можливості для такої системи сигналізації, що дасть змогу власнику на великій дистанції спостерігати за показниками в реальному часі.

У роботі проаналізовано різноманітні види сенсорів, їхні принципи роботи, будову та ефекти, на яких ці сенсори побудовані. До основних можна зарахувати: ємнісний, радіохвильовий і сенсор вібрацій. Саме ці сенсори використовують сучасні системи безпеки і надалі їх використано під час розроблення проєкту.

Суть полягає у розробленні безпровідної системи сигналізації зі зворотним зв'язком, яка могла б працювати на відстані до 100–150 м в умовах природних та штучних завад за невеликої потужності випромінювання.

2. Аналіз та постановка задачі

У сучасному світі багато різноманітних систем сигналізації [1–3]. Їх недоліком є достатньо велика складність встановлення та висока ціна. Також в більшості систем сигналізації використовують один чи два сенсори, це може бути геркон, гіроскоп-акселерометр, сенсор руху тощо. Тому актуальним є розроблення саме мультисенсорної системи, яка б містила не менше ніж три–чотири різні сенсори виявлення вторгнень. Перевагою мультисенсорних охоронних систем, як зазначено раніше, є підвищення імовірності виявлення зловмисника. Розроблювана система призначена передусім для охорони персонального електротранспорту, доволі поширеного сьогодні. Він недешевий, тому його частіше крадуть. Але розроблювана система є універсальною і може використовуватися для охорони інших транспортних засобів та об'єктів.

Для цього у статті запропоновано алгоритм роботи завадостійкої системи сигналізації, що дає змогу побудувати систему, яку практично не можна зламати та подавити. Також буде розроблено відповідну систему сигналізації на сучасній компонентній базі. Система складатиметься з двох пристроїв – брелока та базової станції.

Для досягнення цієї мети потрібно розв'язати такі задачі:

- аналіз типів сенсорів, що можуть використовуватися в системах сигналізації;
- розроблення структурної схеми базової станції безпровідної сигналізації;
- розроблення структурної схеми брелока безпровідної сигналізації;
- розроблення удосконаленого алгоритму шифрування інформації для безпровідної системи завадостійкої сигналізації;
- розроблення алгоритму роботи брелока безпровідної сигналізації;
- розроблення алгоритму роботи базової станції безпровідної сигналізації;
- дослідження технології передавання даних LoRa;
- синтез принципових схем брелока та базової станції безпровідної системи завадостійкої сигналізації;
- розроблення друкованих плат пристроїв безпровідної системи завадостійкої сигналізації;
- розроблення програмного продукту, що забезпечує функціонування системи сигналізації;
- виготовлення макета системи.

3. Основні складові безпровідної системи завадостійкої сигналізації на базі технології LoRa

Для початку означимо терміни, які використовуватимемо у роботі.

Пристрій, який встановлюється на охоронюваний об'єкт, називатимемо базовою станцією. Базову станцію можна буде встановити у власному будинку при вході, на авто чи інший транспортний засіб. У базову станцію інтегровано три сенсори, акумулятор і модуль безпровідного передавання даних LoRa.

LoRa – це технологія, яку використовують модулі безпровідного передавання даних. Ця технологія використовує протокол широкосмугової мережі низької потужності (LPWAN), розроблений компанією Semtech. Він оснований на методах модуляції розширеного спектра. Ця технологія забезпечує належну дальність і мале енергоспоживання. Широкосмугові стільникові технології, такі як 4G та 5G, дають змогу передавати дані на великі відстані. Однак стільникова WAN споживає багато енергії. Абревіатура WAN від англ. Wide Area Network, що в перекладі означає "глобальна мережа". Це комп'ютерна мережа, що охоплює величезні території. Глобальна мережа комунікує цілі мегаполіси, області або навіть держави і містить у собі десятки, сотні, а то і мільйони комп'ютерів [4].

Стільниковий WAN дає змогу передавати великі обсяги даних із високою швидкістю і на великі відстані. Компромісом тут є велике споживання енергії. Якщо нам потрібна бездротова мережа, яка споживає дуже низьку потужність, але також працює на відстані, більші, ніж, скажімо, WiFi, технологія LoRa буде найкращим вибором.

Абревіатура LoRa – від англ. Long Range, що перекладається як "велика відстань". LoRa – це протокол широкосмугової мережі із низькою потужністю. Цей тип бездротового зв'язку призначений для передавання невеликих пакетів даних на великі відстані й працює від акумулятора [5].

Таблиця 1

Порівняння безпровідних технологій за споживаною потужністю [5]

Технологія	Безпровідне з'єднання	Відстань	Споживана потужність, мВт
Bluetooth	Малого радіуса дії	10 м	2,5
Wi-fi	Малого радіуса дії	50 м	80
3G/4G	Стільникове	5 км	5000
LoRa	Енергоефективне	5 км	20

LoRa – це запатентована технологія радіомодуляції, що належить Semtech і займається лише фізичним рівнем стека. Технологія LoRa використовує особливу технологію модуляції Chirp Spread Spectrum – метод зубчастого розширення спектра. Цей метод дає можливість передавання низької потужності на великі діапазони через неліцензійний діапазон ISM. Chirp Spread Spectrum використовує широкосмугові лінійно-частотні модульовані імпульси для кодування інформації.

Відмінна чутливість (до –148 дБм) є ключовою характеристикою LoRa-пристроїв компанії Semtech, що досягається завдяки застосуванню певного методу модуляції. Цей спосіб модуляції передбачає використання технології розширення спектра, за якої дані кодуються широкосмуговими ЛЧМ імпульсами з частотою, що збільшується або зменшується на деякому тимчасовому інтервалі.

На відміну від технології прямого розширення спектра, таке рішення робить приймач стійким до відхилень частоти від номінального значення і спрощує вимоги до тактового генератора. З урахуванням максимальної дозволеної вихідної потужності окремих трансиверів бюджет каналу зв'язку становить 168 дБ, що дає змогу організувати гарантовану лінію зв'язку на відстанях до 15 км у сільській місцевості й до 5 км в умовах щільної міської забудови. Для порівняння: максимально можлива дальність передавання даних інтелектуальних приладів обліку із використанням GFSK-модуляції становить не більше ніж 1–2 км.

LoRa працює у неліцензійному діапазоні ISM на частоті до 1 ГГц. Використання цього діапазону не потребує ліцензії для передавання даних. LoRa працює у неліцензійному радіодіапазоні ISM (промисловий, науковий та медичний), який доступний у всьому світі. Фактична частота цього діапазону ISM для LoRa залежить від країни [5]. В табл. 2 вказано ці діапазони.

Таблиця 2

Частота неліцензійних діапазонів для різних країн [5]

Регіон	Неліцензійна частота, МГц
Азія	433
Європа, Росія, Індія, Африка	863–870
Сполучені Штати Америки	902–928
Австралія	915–928
Канада	779–787
Китай	779–787, 470–510

Аналізуючи зазначене вище, можна зробити висновок, що потужності LoRa модуля 10 мВт цілком вистачить для роботи пристрою на відстані 100–150 м в умовах щільної забудови. Цю відстань вибрано не просто так – це середня відстань, на яку віддаляється брелок (користувач) від базової станції (об'єкта, що охороняється) під час відвідування офісного центру, торговельних комплексів, перебування вдома тощо.

Розглянемо сенсори, які будуть використовуватися в системі. Сенсор, який відповідатиме за найбільшу зону виявлення, – радіохвильовий. Наступний сенсор – ємнісний, що відповідатиме за меншу зону виявлення, але пріоритетність його вища. Останнім сенсором, пріоритет якого найвищий, буде сенсор вібрацій.

Як радіохвильовий сенсор використано модуль RCWL 0516 [6].

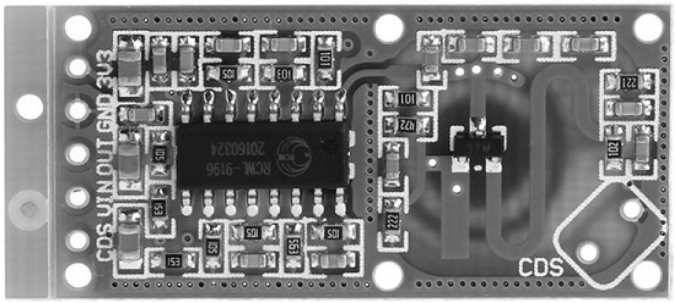
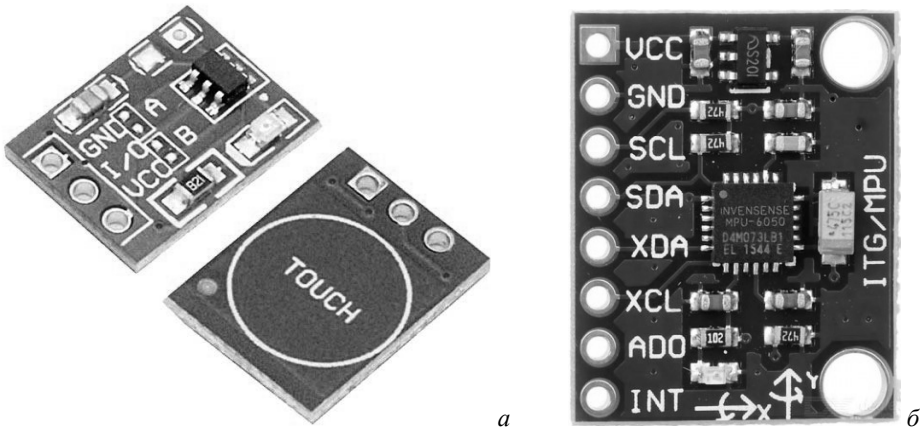


Рис. 1. Радіохвильовий сенсор RCWL 0516

Як ємнісний сенсор використано мікросхему TTP223 [7]. Для детекції вібрацій та переміщення використовується мікросхема акселерометр-гіроскоп MCU-6050 [8]. Модулі, побудовані на базі цих мікросхем, зображено на рис. 2.



а *б*

Рис. 2. Ємнісний сенсор (а) та сенсор вібрацій (б)

Головним центром базової станції є мікроконтролер (MCU). Як для брелока, так і для базової станції запропоновано використовувати мікроконтролер STM32F030 [9], зважаючи на його дешевизну та достатні характеристики для нашого проєкту. За допомогою вищеописаних сенсорів отримують інформацію про об'єкт, який охоронятиметься. Також базова станція повинна мати модуль безпровідного передавання інформації, за допомогою якого будуть відправлятися пакети байтів. Модуль оснований на мікросхемі компанії Semtech SX1276. Для з'єднання може використовуватись інтерфейс SPI чи UART – залежно від типу самого модуля.

У пакет інформації, який буде передаватися між базовою станцією і брелоком, входить інформація, зчитана із сенсорів, а також додаткова інформація. До базової станції ставлять вимоги щодо автономності роботи: вона повинна працювати доволі довго без підзаряджання. Для живлення радіохвильового сенсора потрібен перетворювач напруги, який має бути розташований прямо на платі пристрою. Оскільки базова станція буде встановлюватися на об'єкти, розташовані, зокрема, на вулиці, то потрібно передбачити захист від води не нижче ніж стандарту IP68 [10].

На рис. 3 зображено структурну схему базової станції системи сигналізації.

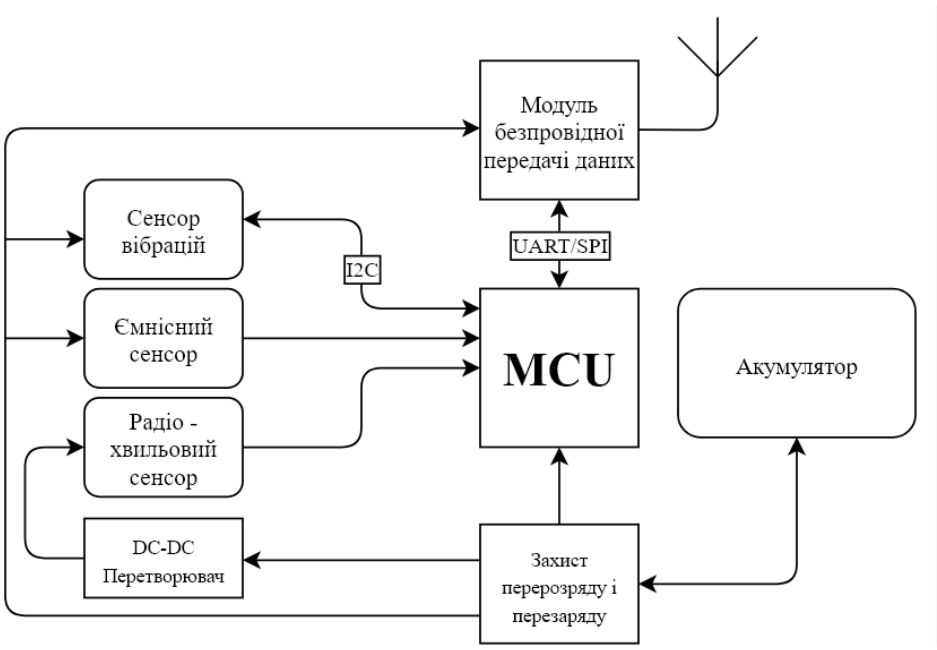


Рис. 3. Структурна схема базової станції

Пристрій, який користувач зможе носити із собою, називатиметься брелоком сигналізації. Брелок сигналізації повинен мати невеликі розміри і вагу. Основою також буде мікроконтролер, згаданий раніше. Оскільки між передаванням і прийманням цілих десять секунд, то частота мікропроцесора може бути невисокою, основну роль повинні виконувати показники енергоспоживання і пам'яті. У брелок входять: п'єзовипромінювач, вібромотор, модуль безпровідного передавання даних LoRa для зв'язку з базовою станцією і дисплей. П'єзовипромінювач вмикається у випадку спрацювання на базовій станції усіх трьох сенсорів або двох пріоритетних, а саме: ємнісного сенсора і сенсора вібрацій. Коли спрацьовує радіохвильовий сенсор, то вмикається вібромотор, що сигналізує користувачеві про наявність якогось рухомого об'єкта на відстані 2 м від його власності. Модуль безпровідного передавання слугує для передавання даних через UART або SPI інтерфейс – залежно від типу модуля. Екран відображає отримані дані. Дисплей повинен мати високу контрастність, мале енергоспоживання, може бути одноколірним, цього цілком достатньо. В майбутньому, зі збільшенням кількості функцій, одноколірного дисплею може не вистачити. Брелок обладнано акумулятором для автономної роботи. Для захисту від розряду і перезаряду акумулятора повинен бути встановлений окремий модуль, який може бути розпаяний прямо на основній платі.

На рис. 4 зображено структурну схему брелока системи сигналізації.

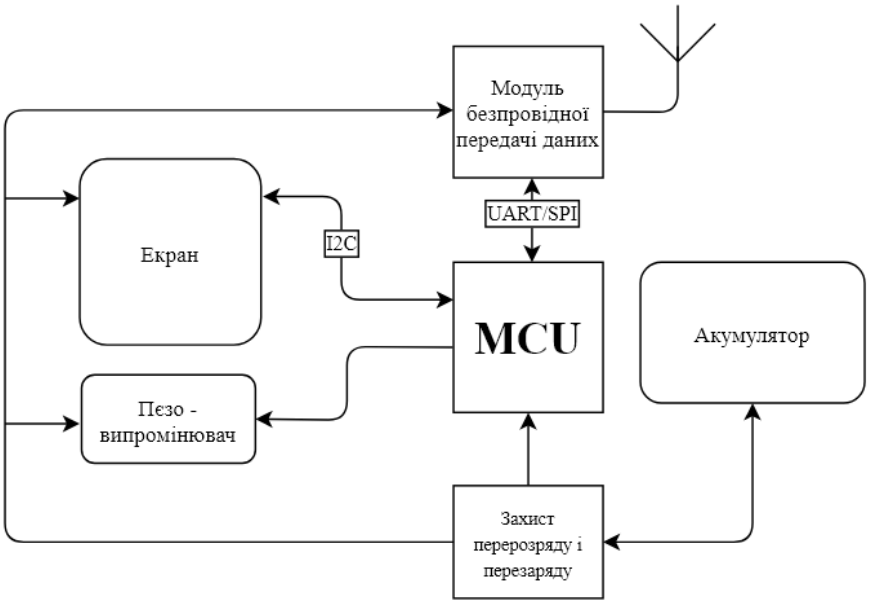


Рис. 4. Структурна схема брелока

4. Алгоритм роботи брелока безпровідної системи завадостійкої сигналізації на базі технології LoRa

Опишемо алгоритм роботи брелока словами, оскільки його блок-схема доволі об'ємна. Робота з пристроєм розпочинається із встановлення базової станції на об'єкт для охорони. Далі потрібно увімкнути спочатку базову станцію, а відтак брелок. У цій системі роль провідного пристрою відіграватиме брелок, тому надсилання пакетів починається з нього. Систему встановлюють у режим охорони, натиснувши на кнопку брелока.

Під час першого увімкнення брелок формує випадковим вибором 64-бітний ключ і 8 випадкових біт для формування унікального пакета для відправки. Цей пакет матиме розмір 32 біт. У відправний пакет з боку брелока входитиме: інформація для керування 8 біт, також випадково згенеровані 8 біт для унікального пакета й останніми будуть 16 біт ключа.

Для коректної обробки інформації і завадостійкості інформаційні біти для керування базовою станцією будуть передані попарно, тобто 4 біти інформаційні й 4 біти для перевірки попередніх чотирьох. Тут може бути записана інформація про ключ, яка його частина тепер передається і будь-яка інформація для керування базовою станцією.

Біти ключа складатимуться з 8 перших біт, раніше згенерованого ключа і 8 додаткових біт для перевірки. Під час наступної відправки буде вибрано наступних 8 біт, а після 8 успішних відправок згенерується новий ключ. Новий 64-бітний ключ передається за допомогою кодування минулим ключем. Час генерації нового ключа залежатиме від кількості успішних передавань.

Випадково згенеровані 8 біт за належного шифрування утворюють суто випадковий пакет, під час кожної відправки і перевідправки він буде різним і таке передавання не можна буде зламати.

Брелок здійснює зв'язок із базовою станцією кожні 10 секунд. Після відповіді базової станції брелок виконує усі операції та переходить у режим сну для збереження заряду акумулятора. Ця процедура триває до 9 секунд, а на 10-й секунді брелок вмикається і негайно починає відправляти дані.

Базова станція може не відповідати на запити брелока через дві причини: сигнал не доходить до базової станції або сигнал блокують. Якщо базова станція не відповідає більше ніж 10 секунд, брелок сигналізує тривогу. Це потрібно для того, щоб унеможливити "заглушення" пристрою, якщо дані не надійдуть на брелок, то він знову через секунду подає запит. Якщо протягом 10 секунд відповіді немає, то вмикається сигналізація на брелоку. В разі спрацювання сенсорів брелок повідомить користувача вібро та звуковим сигналами і на дисплеї відображатиметься інформація,

які сенсори спрацювали. Усі маніпуляції виконують із використанням кодування інформації 64-бітним ключем.

5. Алгоритм роботи базової станції безпровідної системи завадостійкої сигналізації на основі технології LoRa

Опишемо алгоритм роботи базової станції, знову ж таки, словами. Принцип роботи базової станції буде покладено в основу: кодування і декодування прийнятих пакетів від брелока, зчитування даних із сенсорів і вимірювання часу між прийманням і передаванням. Під час першого отримання пакета базова станція записує отримані дані, зчитує інформаційні біти і формує свій пакет для відправки.

У пакет для відправки входитиме: інформація про сенсори 8 біт, інформація про заряд акумулятора 8 біт, а також випадково згенеровані 16 біт для унікального пакета відправки на брелок. Цей пакет зашифрується за допомогою діючого ключа, і дані відправляться просто до брелока.

Якщо цей пакет не дійшов до брелока, то брелок знову відправить попередні дані й базова станція знову сформує новий пакет. У разі повторного відправлення 8 біт ключа не записуються знову, оскільки база звірить їх із попередніми бітами, перевірить час відправлення і визначить, що це перевідправлення даних.

Після успішного передавання даних брелок перевіряє, чи надходить сигнал від брелока. Якщо сигнал надійшов швидше ніж за 9 секунд, то це перевідправлення і ключ не записується. Якщо ж таймер нарахує понад 9 секунд, – це повноцінна відправка. У цьому випадку потрібно: записати ключ, зчитати додаткову інформацію, відправити дані із сенсорів. Базова станція, на відміну від брелока, повинна постійно працювати і перевіряти надходження сигналу, а також показники сенсорів. Якщо якийсь із сенсорів спрацьовує протягом більше ніж 3 секунд, то ця інформація записується в пам’ять і користувач отримає її під час наступної відправки. Після відправки брелок зберігає усі дані сенсорів, а у пам’яті базової станції ці дані обнулюються, коли пакет відправлено до брелока.

У пристрої є три рівні сигналізації. Перший рівень – це виявлення рухомих об’єктів за допомогою радіохвильового детектора. Радіус дії такого детектора не повинен перевищувати 2 м, щоб зменшити імовірність випадкового спрацювання. Другий рівень – це виявлення присутності живого організму за допомогою ємнісного сенсора на віддалі 0,5 м. Третій рівень небезпеки – це виявлення вібрації за допомогою гіроскопа-акселерометра MPU-6050. Звуки та вібрація повинні відрізнятися за інтенсивністю залежно від ступеня ризику для того, щоб користувач міг дистанційно, не дивлячись на екран брелока, оцінити стан ситуації. Відсутність на брелці сигналу, який надсилає базова станція кожні 10 секунд, прирівнюється до третього рівня небезпеки.

6. Розроблення власного алгоритму шифрування безпровідної системи завадостійкої сигналізації на базі технології LoRa

Алгоритм Keeloq [11–13] буде основою для шифрування, але він не може бути ідентичним, оскільки таку систему буде простіше зламати. Отже, модифікуємо його, додавши до результату шифрування кілька перестановок та інверсій, а наприкінці отримані байти можна буде шифрувати ще раз, використовуючи той самий чи навіть інший блоковий шифр.

До отриманого результату можна додати динамічну генерацію ключа і генератор випадкових чисел, який також вноситиме свої дані в пакет. У підсумку отримаємо унікальні пакети для передавання. Перехопити і розшифрувати такі дані майже неможливо.

Після перетворення зашифрована відповідь міститиме 32 біти. У разі зламу зворотне декодування алгоритму навіть за допомогою сучасних комп’ютерів потребуватиме дуже багато часу – понад століття. Схожий алгоритм роботи ще називають діалоговим кодом, брелок ніби веде

діалог із базовою станцією, а біти кожен раз різні. В найближчому майбутньому, швидше за все, навряд чи з'являться пристрої, здатні зламати такий алгоритм.

Удосконалений алгоритм, як зазначено вище, ґрунтуватиметься на блоковому алгоритмі KeeLoq. Спрощену блок-схему алгоритму шифрування показано на рис. 5.

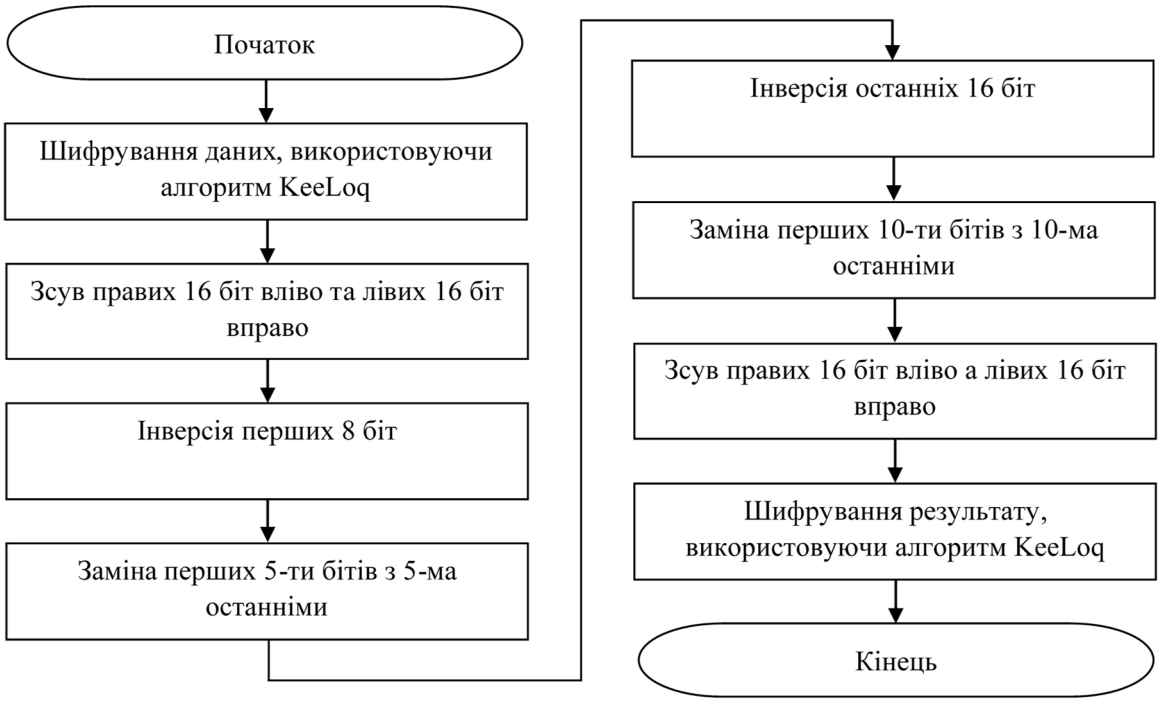


Рис. 5. Спрощена блок-схема удосконаленого алгоритму шифрування

Можна також передбачити цикл, у якому ці дії виконуватимуться декілька разів, але це може позначитись на швидкодії, яка в деяких випадках доволі важлива. Дешифрування потрібно здійснювати у зворотній послідовності.

7. Розроблення друкованих плат брелока і базової станції

Після остаточного вибору усіх компонентів можна спроєктувати схеми та друковані плати, використовуючи усі описані вище компоненти. Для розроблення схем буде використана комплексна система автоматизованого проєктування CircuitMaker (безкоштовний аналог Altium Designer [14]). За допомогою цієї програми можна проєктувати схеми і створювати їх 3D моделі. Принципову схему пристроїв ми не наводимо через обмежений обсяг статті та недоцільність.

На рис. 6 та 7 зображено 3D вигляд друкованої плати брелока із елементами.

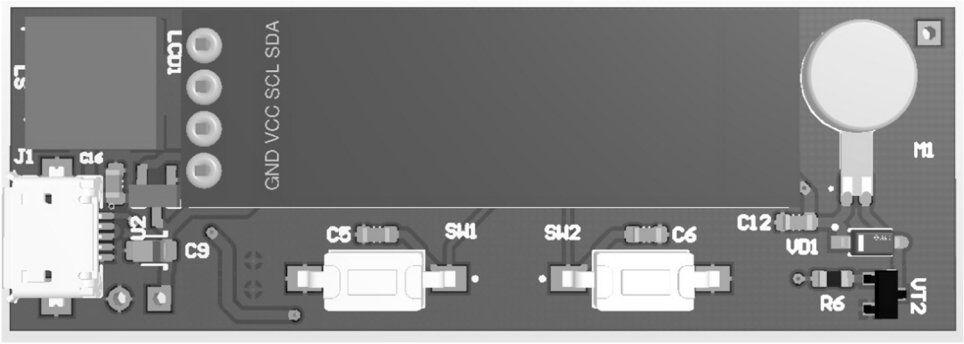


Рис. 6. 3D вигляд друкованої плати брелока з елементами, вигляд зверху

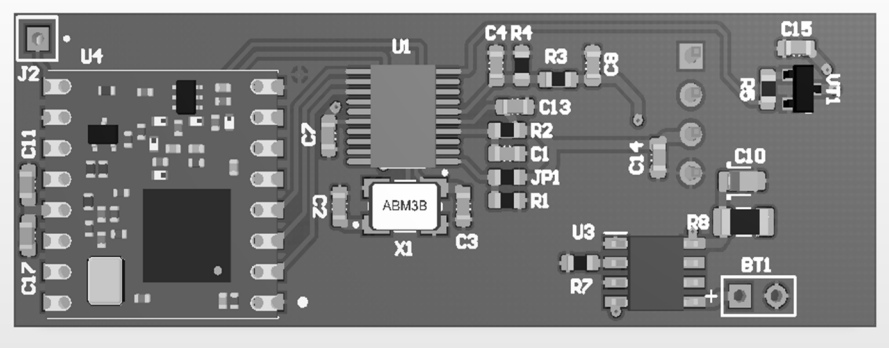


Рис. 7. 3D вигляд друкованої плати брелока з елементами, вигляд зі зворотної сторони

На рис. 8 та рис. 9 зображено 3D вигляд друкованої плати базової станції з елементами.

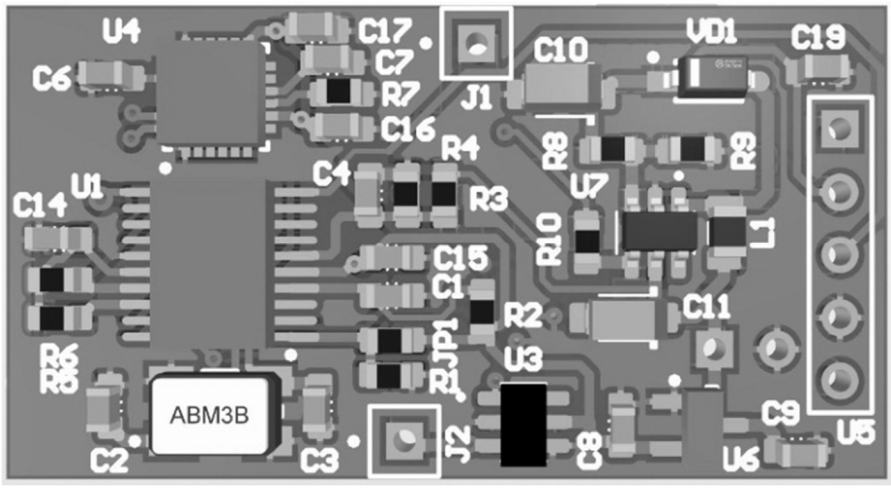


Рис. 8. 3D вигляд друкованої плати базової станції з елементами, вигляд зверху

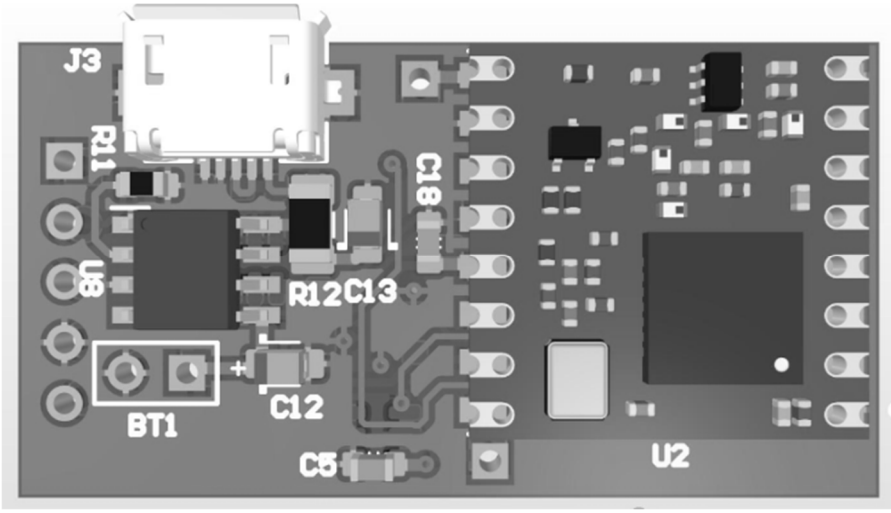


Рис. 9. 3D вигляд друкованої плати базової станції з елементами, вигляд зі зворотної сторони

Радіохвильовий сенсор використовується в цьому випадку як готовий модуль (зображений на рис. 1), підключений до роз'єму U5 для спрощення конструкції.

Після розроблення апаратної та програмної частин пристрою виготовлено макет пристрою. Макет пристрою зображено на рис. 10.

У майбутньому планується виготовлення готового зразку пристрою та подальше дослідження його функціонування, виправлення можливих помилок та додавання нових функцій та можливостей.

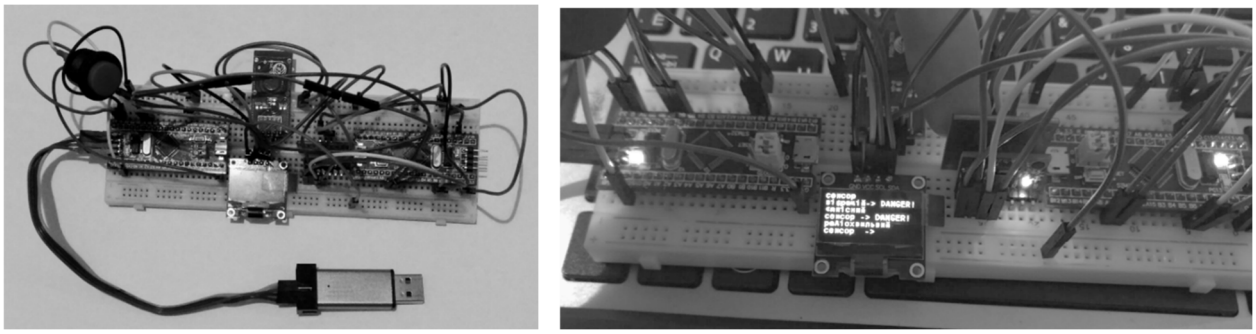


Рис. 10. Макет пристрою

Висновки

Розроблена охоронна система поєднує у собі усі переваги схожих на неї пристроїв. У роботі розроблено принципи функціонування та алгоритми роботи цієї системи. Використана технологія LoRa дуже перспективна і відкриває нові можливості для таких пристроїв, як цей. LoRa завдяки своїй енергоефективності та дальності дії має великі переваги над вузькосмуговими системами передавання даних. У роботі для цієї технології розроблено свої алгоритми передавання даних та шифрування. За допомогою розробленого шифрування можна безпечно передавати дані. Основою шифрування став блочний шифр KeeLog із додатковими модифікаціями, у результаті чого розроблено власний алгоритм, який відмінно шифрує дані та є безпечнішим, ніж основний. Спроєктовано структурні схеми брелока і базової станції. Розроблено принципові схеми та друковані плати для брелока і базової станції. Описано і протестовано основний пакет програм для розроблення програмного забезпечення. Також розроблено макет пристрою із програмним забезпеченням для подальших досліджень, а також готові 3D моделі друкованих плат та принципові схеми пристроїв системи.

Список використаних джерел

[1] K. A. Mamun and Z. Ashraf (2015), "Anti-theft vehicle security system with preventive action", 2015 2nd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE), pp. 1–6.

[2] How Car Alarms Work, available at: https://auto.howstuffworks.com/car-alarm.htm#pt3 (Accessed 8 November 2020).

[3] Common Types of Car Alarm Systems – Automotive Locksmith, available at: https://automotivelocksmiths.com/3-common-types-of-car-alarm-systems/ (Accessed 8 November 2020).

[4] Devalal, Shilpa and Karthikeyan, A. (2018). "LoRa Technology – An Overview", 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), pp. 284–290.

[5] LoRa, available at: https://lora.readthedocs.io/en/latest/#range-vs-power (Accessed 7 December 2020).

[6] RCWL-9196 datasheet, available at: https://img.filipeflop.com › Datasheet_rcwl-0516 (Accessed 7 December 2020).

[7] TTP223 datasheet, available at: https://datasheet.lcsc.com/szlcsc/TTP223-BA6_C80757.pdf (Accessed 7 December 2020).

[8] MPU-6050 datasheet, available at: https://invensense.tdk.com/wp-content/uploads/2015/02/MPU-6000-Datasheet1.pdf (Accessed 7 December 2020).

[9] STM32F030 datasheet, available at: https://www.st.com/resource/en/datasheet/stm32f030f4.pdf (Accessed 7 December 2020).

[10] IEC 60529: Degrees of protection provided by enclosures (IP Code) // International Electrotechnical Commission, Geneva, available at: https://standards.globalspec.com/std/1638833/EN%2060529 (Accessed 10 July 2021)

[11] Eisenbarth, Thomas, Kasper, Timo, Moradi, Amir, Paar, Christof, Salmasizadeh, Mahmoud and T. Manzuri Shalmani, Mohammad (2008), "Physical Cryptanalysis of KeeLoq Code Hopping Applications", IACR Cryptol. ePrint Arch, p. 58.

[12] Eisenbarth, Thomas, Kasper, Timo, Paar, Christof and Indesteege, Sebastiaan (2011), "Keeloq", Encyclopedia of Cryptography and Security (2nd ed.), pp. 671–673.

[13] Gunathilake, Nilupulee A.; Al-Dubai, Ahmed; Buchana, William J. (2 November 2020). "Recent Advances and Trends in Lightweight Cryptography for IoT Security". 2020 16th International Conference on Network and Service Management (CNSM). Izmir, Turkey: IEEE, pp. 1–5.

[14] Altium Designer Documentation, available at: https://www.altium.com/documentation/altium-designer (Accessed 14 December 2020).

DEVELOPMENT OF WIRELESS NOISE-PROOF ALARM SYSTEM BASED ON LORA TECHNOLOGY

S. Fabirovskyy, O. Moskaliuk

Lviv Polytechnik National University, 12, S. Bandery Str., Lviv, 79013, Ukraine

The paper is devoted to the development of a wireless noise-proof system with feedback based on LoRa technology. The relevance of the work lies in the fact that the issue of protecting your property from burglars is always on the agenda. It is also important that the alarm system is universal, it should also be an inexpensive thing that would pay for itself in a short period of time, while at the same time providing a high level of protection. Currently, the next problem is that to buy even a simple protection system you will have to pay well, not only for the device itself, but also for its installation. During installation, the device is connected to the on-board system of the car and this operation also costs a lot, in the future if the purchased system breaks down, you will have to take the car to the service and uninstall everything, while the cut conductors will remain in the car. All this prompts the idea of developing such a system that will not have such disadvantages, which everyone can buy and the installation does not require professional skills, this was the main idea for the paper.

Key words: *LoRa; alarm; STM32; coding; encryption.*