

УДК 004.738

DOI <https://doi.org/10.32838/TNU-2663-5941/2020.3-1/11>**Переверзєв О.А.**Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»**Гумен Т.Ф.**Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»**Трапезон К.О.**Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»**ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ
LPWAN У СУЧАСНИХ СИСТЕМАХ ОХОРОНИ ЖИТЛОВИХ БУДИНКІВ**

Розглянуто найбільш розповсюджені типи топологій з'єднання елементів у розрізі концепції Інтернету речей. Доведено, що найбільш зручною топологією для мережі з низьким електроспоживанням можна вважати топологію типу «зірка». Такий вибір зумовлений простотою реалізації архітектури мережі на основі концепції Інтернету речей та широкими можливостями з модернізації мережі, у зв'язку з відповідним налагодженням та функціонуванням пристроїв мережі. Іншою перевагою такого підходу є критерій мінімального електричного споживання системи. Проаналізовано фізичний та каналний режими системи пристроїв на основі Low Power Wide Area (LPWA). За результатами аналізу виявлено, що технологія LPWA за прийнятим протоколом використовує неліцензійну смугу радіочастот і загальнодоступний протокол, а це своєю чергою створює можливості до спроб зовнішнього втручання в мережу. Зловмисник може прослуховувати адресу легального терміналу і генерувати підроблені пакети на шлюз, щоб викликати перевантаження ланки мережі. Наведено класифікацію класів кінцевих пристроїв, які працюють в рамках технології LPWAN. Знайдено, що найбільш зручним за енергоефективністю та повною сумісністю з сенсорами IoT є клас А пристроїв. Запропоновано алгоритм, за яким можуть функціонувати окремі LoRA-модулі системи задля забезпечення принципу мінімального споживання електричної енергії.

Як практичне спрямування дослідження наведено варіант архітектури системи безпеки будівлі на основі LoRa-модулів. Ця архітектура вирізняється модульністю підключених пристроїв і може бути розширена шляхом підключення нових IP-камер без переналагодження зв'язків інших елементів з постом охоронної сигналізації. Надані рекомендації з архітектури мережі в рамках дослідження можуть забезпечити надалі під час реалізації підвищений рівень надійності роботи елементів системи охорони житлового будинку. Загалом же проведене дослідження та окремі його пункти можуть слугувати основою для модернізації наявних систем охорони будівель, де управління та моніторинг стану об'єкту реалізовано на основі збору даних від контрольних пристроїв приміщення з подальшим їх пересиланням на пульт безпеки системи.

Ключові слова: клас, LPWAN мережі, РНУ рівень, передача даних, LORA-модулі, смуга частот, енергоспоживання, архітектура мережі, шлюз.

Постановка проблеми. Зі збільшенням кількості підключених пристроїв в Інтернеті речей (IoT) зростають паралельно вимоги і до підключення цих пристроїв (наприклад, ресурсу акумулятора, вартості розгортання та покриття) для забезпечення ефективної комунікації між цими пристроями. Нові технології малої потужності (LPWA) відкривають шлях для розв'язання проблеми, оскільки вони можуть забезпечити доступне підключення до пристроїв з малим енер-

госпоживанням на дуже великих площах. Загальновідомо, що в класичних схемах розгортання систем охорони приміщень ситуація з управлінням ще більше може ускладнюватись з технічного боку, коли необхідно збільшити не лише кількість контрольних точок для моніторингу (наприклад, з системи відеоспостереження забезпечити повну відсутність сліпих зон), але й забезпечити при цьому різні види інформації з моніторингу об'єкту. І тут йдеться не лише про сенсори диму,

руху, але й потрібна інформація, яка забезпечує автоматичні функції роботи систем та комунікацій будинку. Наприклад, необхідно, щоб у будинку, який знаходиться під охороною, світло в певній кімнаті вмикалось і вимикалось в певний часовий інтервал доби. І при цьому, зрозуміло, щоб наявні сенсори охорони не спрацьовували на хибний сигнал тривоги. Інша ситуація може бути пов'язана з поливом рослин або годуванням через певний електронний механізм домашніх тварин. Вочевидь, у класичній системі безпеки будинку такі додаткові функції забезпечити вкрай важко. Одним із можливих рішень у цьому напрямку може стати використання технологій у рамках концепції «розумного» будинку і IoT.

Постановка завдання. LPWAN – це абревіатура для «малопотужної широкопasmової мережі», типу радіотехнології, яка використовується для безпроводового передавання даних у додатках IoT [1]. Це не окрема технологія, а група різних технологій безпроводової мережі. LPWAN можуть використовувати ліцензовані або неліцензовані частоти та включати власні або відкриті стандарти. І тому основним завданням статті можна визначити те, щоб спроектована система безпеки будинку вирізнялась тим, що її елементи повинні відповідати стандартизованим технологіям та рівням концепції Інтернету речей. Додатковою ознакою слід визна-

чити той факт, щоб система охорони забезпечувала б довготривалу автономність роботи її елементів – сенсорів, камер, перемикачів тощо.

Метою статті є визначення ключових особливостей, які слід враховувати під час використання технології малої потужності на різних етапах проектування систем безпеки будинків на основі LORA-модулів IoT. Додатково слід відмітити в дослідженні пошук алгоритмів і підходів до створення телекомунікаційної системи на основі технології LPWAN для Інтернету речей.

Виклад основного матеріалу дослідження. Є величезна кількість топологій IoT для мереж, основним завданням яких є передавання різного роду інформації. Але найбільш поширеним серед них є сітчаста (mesh) топологія, зіркоподібна топологія та двоточкова топологія. Більшість технологій глобальної мережі з низьким енергоспоживанням (LPWAN) на доповнення до WiFi та стільникових мереж використовують топологію зіркоподібної мережі. Так, мережа типу «зірка» має у своїй архітектурі маршрутизатор або точку доступу в середині топології, яка своєю чергою підключається до всіх терміналів або вузлів мережі (рис. 1).

Як мобільні модулі передавання даних виступають мобільні гаджети, які дозволяють приймати, передавати та накопичувати та відображати

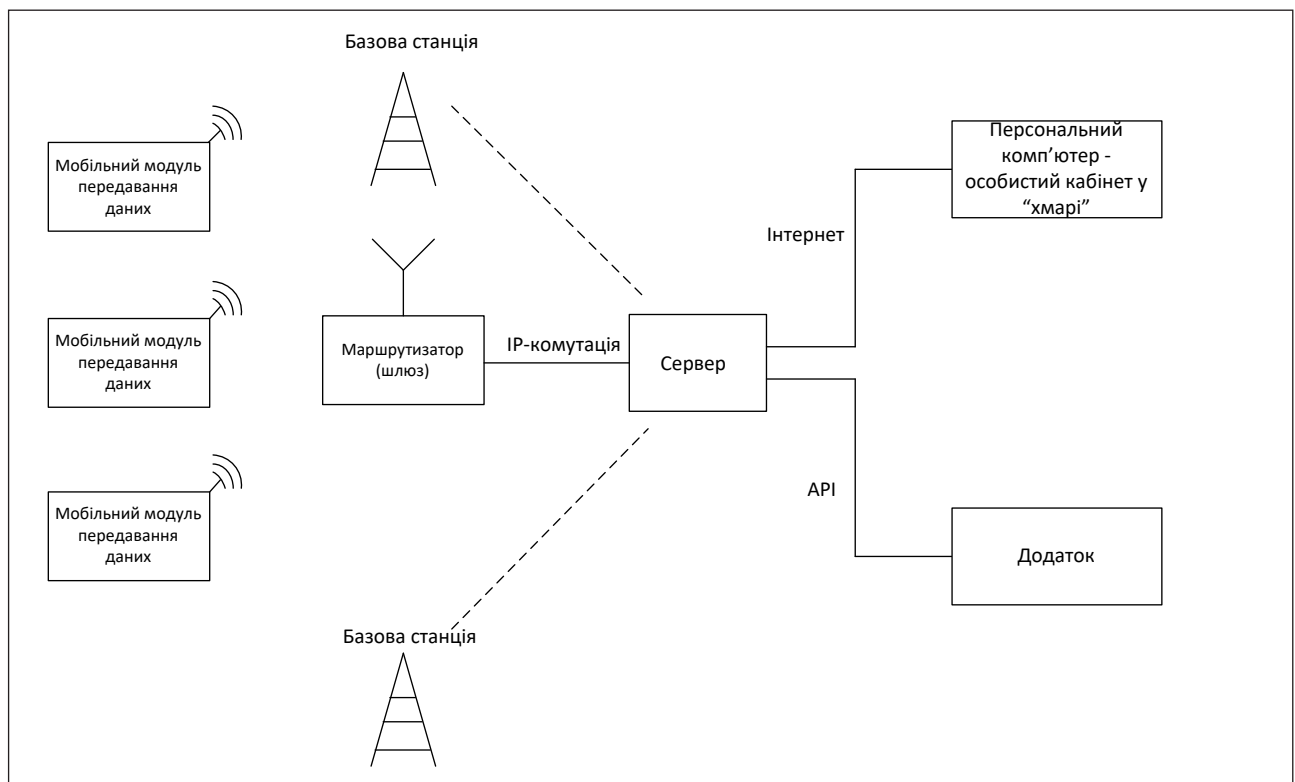


Рис. 1. Топологія мережі LPWAN

інформацію з датчиків, безпроводових відеокамер та сенсорів у комплексі архітектури системи безпеки будинку. У найпростішому випадку це може бути смартфон з відповідним програмним забезпеченням на Android або iOS. У рамках технології LPWAN наведена топологія дозволяє підключення нових кінцевих пристроїв, і їх кількість не визначається рівнем енергоспоживання останніх. Завдяки одноранговому з'єднанню «точка – точка» топологія «зірка» значно простіша і дешевша в реалізації у порівнянні з топологією сітки (mesh). Безпека мережі також зростає, оскільки кінцеві точки працюють незалежно одна від одної. Якщо вузол атакований, інша частина мережі все ще залишається неушкодженою. Крім цього, слід відмітити, що така топологія підключення пристроїв дозволяє розвантажити сервер, адже колізії в цьому разі майже неможливі через особливості роботи базових станцій мережі. Оскільки в цьому разі передбачається активною функція перемикачів частотних каналів у неліцензованому діапазоні частот. Крім цього, аналізуючи топологію на рис. 1, варто відзначити про незалежність роботи особистого кабінету з управління системою, який до того ж знаходиться у хмарному середовищі. Такий підхід значно ускладнює стороннє втручання до роботи системи через те, що дані управління від адміністратора проходять через рівень шифрування, і мережа Інтернет в цьому разі використовується як «транспортний» засіб передавання інформації. Окремо слід відзначити і незалежне розміщення додатку Application (API), який регламентує принципи та підходи підключення нових елементів до мережі на основі технології малої потужності. В цьому разі зміна топології мережі LPWAN через підключення нових елементів до базової станції не передбачає зривання наявних з'єднань або не призводить до перезавантаження всієї системи на основі LPWAN. Такий принцип функціонування дозволяє значно подовжити час автономної роботи сенсорів, датчиків та кінцевих пристроїв системи безпеки будинку, які підключені до мережі LPWAN. Таким чином, мережі типу «зірка» LPWAN оптимізовані для мінімального енергоспоживання і можуть забезпечити тривалий термін служби батареї на стороні датчика. На відміну від топології сітки, вузли не обов'язково повинні бути постійно активними для прослуховування і ретрансляції даних від інших вузлів. Поза часом передавання вони можуть переходити в «сплячий режим» і практично не споживати енергію.

Основним недоліком топології «зірка» є те, що площа мережі обмежена максимальною даль-

ністю передавання між пристроями і шлюзом [2]. Задля визначення особливостей роботи LPWAN розглянемо в рамках дослідження фізичний (PHY) та MAC-рівні елементів за технологією LPWAN.

Фізичний та MAC-рівні LoRa-модулі

Телекомунікаційна система збору інформації з підтримкою технології LPWAN складається з декількох компонентів, які традиційно можна описати на основі взаємодії різних рівнів роботи. Фізичний (PHY) рівень на рівні підключення апаратури визначає характеристики для передавання даних між елементами мережі. Натомість каналний рівень відповідає за виявлення змін на фізичному рівні і створення протоколу для відправлення даних. Відмітимо, що в основі роботи за технологією LPWAN виділяють поняття LoRa – це запатентований формат модуляції, який належить Semtech. LoRa модулі використовують техніку модуляції «лінійно-частотна модуляція-спектром (CSS)» для формування фізичного (PHY) рівня технологічного стеку (рис. 2). Крім цього, в основі роботи закладено метод розширеного спектра для передавання даних за різними частотним каналам і з різними швидкостями, так що шлюз може адаптуватися до мінливих умов і оптимізувати спосіб обміну даними з кожним пристроєм.

Пристрої LoRa вирізняються такими особливостями, як великий радіус дії, низьке енергоспоживання і безпечна передача даних для додатків IoT. Один шлюз може взаємодіяти з декількома сотнями тисяч пристроїв на відстані до 32 кілометрів на безперешкодному середовищі. Ці технології забезпечують більшу дальність, ніж стільникові мережі, і можуть використовуватися в громадських, приватних або гібридних мережах.

Недоліком є те, що технологія LoRa вибирає неліцензійну смугу частот і загальнодоступний протокол, який створює вразливість у мережі. Зловмисник може прослуховувати адресу легального терміналу і генерувати підроблені пакети на шлюз, щоб викликати перевантаження ланки мережі [3]. Загалом же мережа LPWAN, за винятком перевантаженої ланки, все одно залишається працездатною.

Архітектура мережі LoRaWAN складається з кінцевого пристрою (ED), шлюзу (GW), мережного сервера (NS), сервера додатків (AS) і сервера приєднання (JS). Такий варіант архітектури є фактично удосконаленою версією архітектури, яка показана на рис.1 для LPWAN. Так, у цьому разі роль базової станції для підключення елементів до мережі відіграє шлюз доступу. Крім цього, на цьому рівні обладнання змінюються

права відповідальності з функціонування мережі. А це накладає певні особливості з регламентації роботи мережі LoRaWAN, адже рівень доступу через відповідні шлюзи є кінцевим елементом до підключення до мережі Інтернет в рамках IoT. І у разі його несправності може бути повністю відключена можливість віддаленого моніторингу і управління мережею LoRaWAN. Таким чином, повідомлення передаються між кінцевим пристроєм та сервером-шлюзом. Шлюз отримує доступ до мережного сервера через стандартне IP-з'єднання, а кінцевий пристрій обмінюється даними з одним або декількома шлюзами за допомогою однопрохідного LoRa-модуля.

На підставі роботи рівня MAC LoRa в LoRaWAN можна виділити три класи кінцевих пристроїв. Класи допомагають класифікувати пристрої на основі типу з'єднання, яке, по суті, визначає його енергоспоживання і доступність висхідної лінії зв'язку і низхідної лінії зв'язку. Класи визначені за принципом перших літер латинського алфавіту – клас А, клас В і клас С (рис. 2). Ці три різних класи пристроїв призначені для забезпечення різних потреб у широкому діапазоні додатків. Всі три класи підтримують двосторонній зв'язок [4; 5]. Найбільш зручним за енергоефективністю та повною сумісністю з сенсорами IoT є клас А пристроїв. На противагу цьому, клас С пристроїв, навпаки, за умови досягнення максимального рівня прийому даних визначається значним споживанням електроенергії. Зазначимо, що вибір класу пристроїв в LoRaWAN пов'язаний з особливостями з'єднання між пристроями мережі та безпосередньо визначається конфігурацією створеної мережі IoT, інтервалами передавання даних та власне типом цих даних. Так, якщо необхідно передавати зображення з IP-камери в режимі

реального часу в системі безпеки будинку цілодобово, то тут, вочевидь, бажано класифікувати пристрої за класом С. В іншому разі, коли інформація збирається з сенсорів руху в приміщенні IoT-системи будинку, то в межах LoRaWAN такі пристроїв відносять до класу А.

Система охорони житлового будинку на основі LPWAN

Технологія LPWAN має глибоку проникність для підключення всередині приміщень. Під час використання систем безпеки, обладнаних за технологією LoRa, як запобіжний захід стратегічно розміщуються домофони, камери відеоспостереження, датчики сигналізації дверей і вікон та автоматичні дверні замки (рис. 3). Це дозволяє власнику помешкання захистити себе від потенційних загроз. Вся система може керуватися зі смартфона в будь-який час.

Аналіз архітектури за рис. 3 є практичним відображенням архітектури, яка показана на рис. 1. Так, у цьому разі функції управління системою приймає на себе пост охоронної сигналізації, який може бути реалізований повністю в автономному режимі роботи. Через те, що така архітектура передбачає підключення до мережі Інтернет, то центральна станція моніторингу може бути віддалена на значну відстань від місця знаходження будинку. Крім цього, на основі LoRa-модулів є можливість у розробників виділити центральну станцію моніторингу і мобільний додаток API в окремий модуль. Тим самим, архітектура в частині її управління значно спрощується. Особливо це стосується, коли наведена архітектура може бути реалізована не для однієї системи безпеки будинку, а для декількох окремих приміщень в межах приміського коттеджного містечка. За такої технічної реалізації система управління на

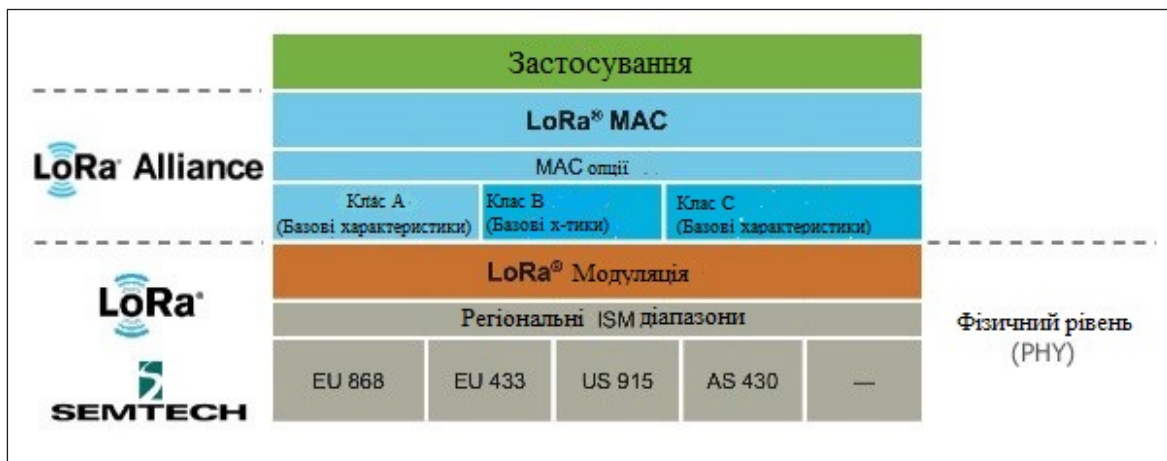


Рис. 2. Типова системна архітектура кінцевого пристрою LoRaWAN

програмному та апаратному рівнях може бути єдиною. Загалом функціонування LoRa-активованої системи безпеки можна поділити на такі частини:

- двері, вікна та датчики руху викликають сигнали тривоги у разі виявлення руху;
- безпроводові сирени і камери безпеки активуються датчиками;
- управління даними здійснюється за допомогою гібридних шлюзів LoRaWAN і Wi-Fi;
- шлюз передає інформацію в хмару або на мережевий сервер, а потім дані обробляються;
- аварійні сигнали активуються на основі оброблених даних;
- смартфони і пристрої отримують оповіщення.

Аналізуючи такий підхід, слід відмітити, що шлюзи доступу в системі можуть бути підключені і до стільникової мережі, а можуть використовуватися і в громадських, приватних або гібридних мережах.

Крім цього, варто відмітити, що передавання інформації через шлюз проходить без аналізу даних. А це своєю чергою може призвести до передавання фішингової інформації, яка значно буде ускладнювати роботу мережного серверу. Через це рекомендується або сервер реалізувати на програмному рівні з функцією аналізу даних та віддаленим розташуванням апаратної частини, або на лінії від передавання даних забезпечити моніторинг інформації перш ніж дані потраплять або у сервер хмарного середовища, або до іншого елемента мережі. Іншим способом захисту мережі та даних, які передаються в системі безпеки, є введення багаторівневого шифрування інформації. Причому в цьому разі необхідно забезпечити захист на основі ключів, які прив'язані до фізичних MAC-адрес кінцевих пристроїв, серверів та

шлюзів доступу. Зрозуміло, що надійність мережі в такому разі значно підвищується, але можуть виникнути труднощі у разі розширення мережі на основі LoRa-модулів. Оскільки в такому разі необхідно мати інструменти додавання елементів та їх злагодженої шифрованої роботи з іншими пристроями мережі.

Нові технології LPWAN працюють на частотах, включених у безлімітні смуги ISM (промислові, наукові, медичні). Тому, на відміну від операторів мобільного зв'язку, операторам мережі LPWAN не доводиться купувати дорогі ліцензії для призначення смуг радіочастотного спектра. LoRaWAN - це специфікація LPWAN, яка дозволяє пристроям на батарейках підключатися до мережі IoT на великі відстані, з низькою пропускну здатністю, в регіональній, національній або глобальній мережі. Мережі LPWAN будуть широко поширені у світі Інтернету речей, особливо там, де потрібна покриття в кілька кілометрів і низьке енергоспоживання.

Висновки. Визначено ключові необхідності використання технології малої потужності (LPWA) під час створення мереж на основі Інтернету речей. Зазначено, що основною топологією мережі, де наявна окреслена технологія є топологія зіркоподібної мережі. Такий вибір зумовлений простотою реалізації мережі на основі IoT та економічними розрахунками, пов'язаними з налагодженням та функціонуванням пристроїв мережі. Іншою перевагою такого підходу є критерій мінімального електричного споживання з боку кінцевих пристроїв системи та транзитних елементів.

Проаналізовано фізичний та каналний режими системи пристроїв на основі LPWA. За результатами аналізу виявлено, що LoRa-модулі в рамках LPWAN використовують неліцензійну смугу



Рис. 3. Архітектура безпеки будівлі на основі залучення LoRa-модулів

радіочастот і загальнодоступний протокол, який «створює» можливості до появи вразливості в роботі мережі. Зловмисник може прослуховувати адресу легального терміналу і генерувати підроблені пакети на шлюз, щоб викликати перевантаження. Наведено класифікацію класів кінцевих пристроїв, які працюють у рамках технології LPWAN. Знайдено, що найбільш зручним за енер-

гоефективністю та повною сумісністю з сенсорами IoT є клас А пристроїв. Як практичне спрямування дослідження описано архітектуру безпеки будівлі на основі LoRa-модулів. Ця архітектура вирізняється модульністю підключених пристроїв і може бути розширена шляхом підключення нових IP-камер без перенастроювання зв'язків інших елементів з постом охоронної сигналізації.

Список літератури:

1. Ли П. Архитектура интернета вещей. Москва : «ДМК Пресс», 2019. 454 с.
2. McEwen A. Designing the Internet of Things, USA : Publishing NT, 2013. 336 p.
3. Сети LPWAN: история и перспективы. URL: <http://orion-m2m.com/ru/news/seti-lpwan-istoria-i-perspektivy/> (дата звернення: 02.05.2020).
4. Кучерявый А.Е. Самоорганизующиеся сети. Санкт-Петербург : «Любавич», 2011. 312 с.
5. Jerker D. IoT Automation: Arrowhead Framework, Great Britain : CRC Press, 2017. 366 p.

Pereverziev O.A., Humen T.F., Trapezon K.O. RESEARCH OF FEATURES OF USING LPWAN TECHNOLOGY IN MODERN HOUSEHOLD SECURITY SYSTEMS

The most common types of topologies of connection of elements in the context of the concept of the Internet of Things are considered. It is proved that the most convenient topology for a network with low power consumption can be considered a topology of the "star" type. This choice is due to the simplicity of the network architecture based on the concept of the Internet of Things and the wide range of opportunities for network modernization, due to the appropriate setup and operation of network devices. Another advantage of this approach is the criterion of minimum electrical consumption of the system. The physical and channel modes of the Low Power Wide Area (LPWA) device system are analyzed. According to the results of the analysis, the LPWA technology according to the adopted protocol uses an unlicensed radio frequency band and a publicly available protocol, which in turn creates opportunities for attempts to externally interfere with the network. An attacker could eavesdrop on the address of a legal terminal and generate fake packets on the gateway to cause network overload. The classification of classes of end devices operating within the framework of LPWAN technology is given. It was found that the most convenient in terms of energy efficiency and full compatibility with IoT sensors is class A devices. An algorithm is proposed according to which separate LoRa-modules of the system can function in order to ensure the principle of minimum electricity consumption.

As a practical direction of the study, a variant of the architecture of the building security system based on LoRa-modules is given. This architecture is characterized by the modularity of the connected devices and can be extended by connecting new IP-cameras without reconfiguring the connections of other elements with the security alarm post. The provided recommendations on the architecture of the network in the study can provide in the future with an increased level of reliability of the elements of the security system of a residential building. In general, the study and some of its points can serve as a basis for modernization of existing building security systems, where management and monitoring of the object is implemented on the basis of data collection from control devices and then forwarded to the system security panel.

Key words: class, LPWAN network, PHY level, data transmission, LORA modules, frequency band, power consumption, network architecture, gateway.