Автоматизація та інформаційні технології в природокористуванні
Automation and information technology and nature management

УДК 004.738.5:005 https://doi.org/10.37700/enm.2021.3(21).127 - 135

Автоматизована система передачі даних про стан об'єктів критичної інфраструктури із застосуванням сучасних інформаційно-телекомунікаційних технологій

С.М. Чумаченко [1], А.С. Парталян [2], А.О. Мошенський [3], М.Л. Сукало [4], Л.Д. Філатова [5]

[1, 3, 4] Національний університет харчових технологій, (м. Київ, Україна)
[2] Міністерство оборони України, (м. Київ, Україна),
[5] Харківський національний університет імені В.Н. Каразіна, (м. Харків, Україна)
email: [1] s_chum@ukr.net, [2] partandrej@gmail.com, [3] ut5uuv@yandex.ua,
[4] biginhunter@gmail.com, [5] filatovald@ukr.net; ORCID: [1] 0000-0002-8894-4262;
[2] 0000-0001-7149-8975; [3] 0000-0002-4584-4958; [4] 0000-0003-3437-8290;
[5] 0000-0002-6605-3442

В статті приведено результати дослідження авторів щодо застосування сучасних інформаційно-телекомунікаційних технологій для передачі моніторингової інформації про стан об'єктів критичної інфраструктури. На сьогоднішній день ці об'єкти є ключовими для роботи систем життєзабезпечення країни та підтримки на належному рівні техногенної і кібербезпеки існуючої інфраструктури. Велике значення в умовах росту техногенних аварій і катастроф приділяється розробці сучасних підходів для системи попередження та моніторингу надзвичайних ситуацій на потенційно небезпечних об'єктах критичної інфраструктури. Значні зусилля зосереджуються на створенні реальних технічних рішень побудови бездротових сенсорних мереж з використанням інтелектуальних моніторингово-сигнальних датчиків, безпілотних літальних апаратів і геоінформаційних технологій для забезпечення оперативного моніторингу таких об'єктів та прилеглих територій.

Однією із ключових компонент такої технології є телекомунікаційна, що базується на нових підходах до реконфігурації радіомереж. Середовищем надійної передачі даних про стан об'єктів критичної інфраструктури може бути безпроводова радіомережа, яка буде функціонувати в складних умовах надзвичайних ситуацій. Враховуючи значну насиченість радіопростору задля уникнення взаємних завад треба орієнтуватися на регіональні стандарти, серед яких слід виділити LoRaWAN, що був розроблений компанією LoRa Alliance у 2015 році для забезпечення з'єднання з низьким енергоспоживанням для кінечних пристроїв, які працюють від акумуляторів.

В статті деталізовано протоколи стандарту LoRaWAN та ключові підходи до розробки різних топологій таких радіомереж для регіонів Європи, США і Австралії. Проведено аналіз топологій безпровідних сенсорних мереж і їх прикладного застосування для створення різних радіомереж. Цільовими клієнтами таких радіомереж є об'єкти критичної інфраструктури, наприклад атомні електростанції, регіональні сховища радіоактивних відходів, небезпечні хімічні виробництва й інші потенційно-небезпечні об'єкти, та служби ДСНС, що займаються моніторингом радіаційної й хімічної обстановки тощо.

Ключові слова: *критична інфраструктура, діапазон частот, ретрансляція, маршрутизатор, пропускна здатність.*

Актуальність статті обумовлена необхідністю забезпечення оцінювання та прогнозування ризиків і загроз виникнення надзвичайних ситуацій природного, техногенного та військового характеру на об'єктах критичної інфраструктури, а також недосконалістю існуючих програмно-апаратних комплексів, що застосовуються підрозділами оперативно-рятувальної служби цивільного захисту ДСНС України.

Захист критичної інфраструктури зачіпає питання національної безпеки, і тому входить до компетенції держави. Тим не менше, велика її частина знаходиться у власності приватного бізнесу, тому держава і бізнес змушені спільно нести відповідальність за безпеку і стабільне функціонування. Під критичною інфраструктурою (КІ) є такі засоби, обладнання, мережі та служби, які, у разі їх пошкодження чи руйнування, будуть мати значний вплив на здоров'я, безпеку, економічний стан чи ефективне функціонування держави. Така інфраструктура, у разі її незахищеності, може бути вразливою до впливу катастроф

природного характеру чи техногенних аварій, спричинених діяльністю людини, а також бойових дій і терористичних атак.

Захист критичної інфраструктури базується на збереженні функціональності, стійкості та надійності таких інфраструктур. Це комплексний захід, що виходить за межі національних кордонів, зважаючи на інтегрованість та взаємозалежність нашого і європейського суспільств, включаючи наступні складові - енергетичне постачання, засоби зв'язку, транспортні мережі тощо. Ураження критичної інфраструктури в одній країні може мати серйозний вплив та негативні наслідки цілого ряду країн, що її оточують, з подальшими каскадними наслідками типу ефектів «доміно».

Аналіз публікацій. В ЄС спроба визначити КІ була здійснена в 2005 р. шляхом підготовки «зеленої книги» [1], згідно з положеннями якої до КІ було включено 11 секторів. Згодом Директивою Європейської Комісії № 114 2008 р. [2] лише два сектори були визнані пріоритетними – це енергетика (електромережі та об'єкти із генерування та передачі електроенергії; нафтовидобувна та нафтопереробна промисловість, нафтопроводи та сховища; газовидобувна промисловість, газопроводи, термінали зрідженого газу) та транспорт (автодорожній, залізничний, авіаційний транспорт; річковий, океанічний і морський флот; порти).

Основний зміст. При визначенні елементів КІ будується ієрархія критеріїв, що охоплює такі основні групи: економічна безпека (значна частка продукції на ринку, велика кількість зайнятих співробітників, великий платник податків); безпека життєдіяльності та здоров'я населення (забезпечення роботи аварійно-рятувальних служб, екстреної допомоги населенню; недопущення техногенних аварій регіонального або національного масштабів); державна безпека і оборона (недопущення порушення керованості державою, зниження боєздатності збройних сил, розголошення таємної інформації); національна самоповага та імідж держави (збереження культурних цінностей, авторитету держави). Наприклад, згідно із вищезгаданою Директивою Європейської Комісії при визначенні потенційних елементів критичної інфраструктури враховують такі фактори та характеристики [2]:

– масштаб (географічне охоплення території, для якої втрата елементу критичної інфраструктури викликає значну шкоду);

– важкість можливих наслідків за такими показниками:

а) вплив на населення (число постраждалих, загиблих, осіб, які отримали серйозні травми, а також чисельність евакуйованого населення);

б) економічна шкода (вплив на ВВП, розмір економічних втрат, як прямих, так і непрямих);

в) екологічна шкода (вплив на населення та навколишнє природне середовище);

г) взаємозв'язок з іншими елементами критичної інфраструктури;

д) політичний ефект (втрата впевненості в дієздатності влади);

е) тривалість впливу (як саме і коли проявлятимуться наслідки, пов'язані з втратою чи відмовою об'єктів критичної інфраструктури).

Процес визначення елементів критичної інфраструктури включає оцінювання загроз та ризиків для об'єктів, спричинених факторами різного походження (техногенного, природного та соціально-політичного характеру) та аналіз взаємозалежностей між цими елементами [3]. Вказане потребує проведення ґрунтовних наукових досліджень, а також розробки та впровадження відповідних інформаційних технологій для їх моделювання із використанням геоінформаційних технологій [4].

Технологія екологічного моніторингу й оцінки ризиків у зоні спостереження потенційно-небезпечних об'єктів із застосуванням інтелектуальної сенсорної техніки являє собою сукупність технічних рішень побудови бездротових сенсорних мереж з використанням моніторингово-сигнальних датчиків, безпілотних літальних апаратів і геоінформаційних технологій [5].

В першу чергу, краудсорсингова система використовує потенціал множинного доступу соціально активних людей до інформаційних мереж і забезпечує оперативний екологічний моніторинг і залучає сучасні технічні засоби аналізу інформації, а саме: інтелектуальні сенсори (дозиметри, газоаналізатори, сейсмічні датчики та ін.), безпровідні сенсорні мережі, відеореєстратори з інтелектуальною платформою виявлення терористичної загрози, мобільні пристрої, супутниковий моніторинг, інтернет та аероплатформи з БПЛА.

Розглянемо структурно-функціональну схему даної системи (рис. 1) [5]. Слід зазначити, що джерелами інформації можуть бути не тільки інтелектуальні датчики БСМ, але й різноманітні персональні пристрої: телефони, смартфони, планшети, відеокамери, а також бортове обладнання БПЛА або космічних супутників Землі. Для того, щоб зібрати та обробити такий великий обсяг інформації розроблено архітектуру потужного центру обробки даних (ЦОД), що оснащений відповідними серверами.

Спочатку дані через мережу Інтернет або виділені канали потрапляють на внутрішній сервер, потім обробляються працівниками центрального або регіональних кризових центрів, а потім публікуються на зовнішньому сервері. В залежності від типу даних, що надходять, для обробки використовується відповідні сервери: сервер ГІС, сервер обробки потокових даних, сервер відеоаналітики, почтовий, файловий і сервер відеоконференцій.

Технологічний продукт дозволяє вирішувати такі важливі проблеми, як дистанційний 3D моніторинг зони спостереження за екологічною обстановкою, оцінка ризиків впливу потенційно-небезпечних об'єктів на здоров'я людей, що проживають у зоні спостереження, забезпечення інформаційно-телекомунікаційних послуг у районах зі зруйнованою або відсутньою інфраструктурою [6, 7].

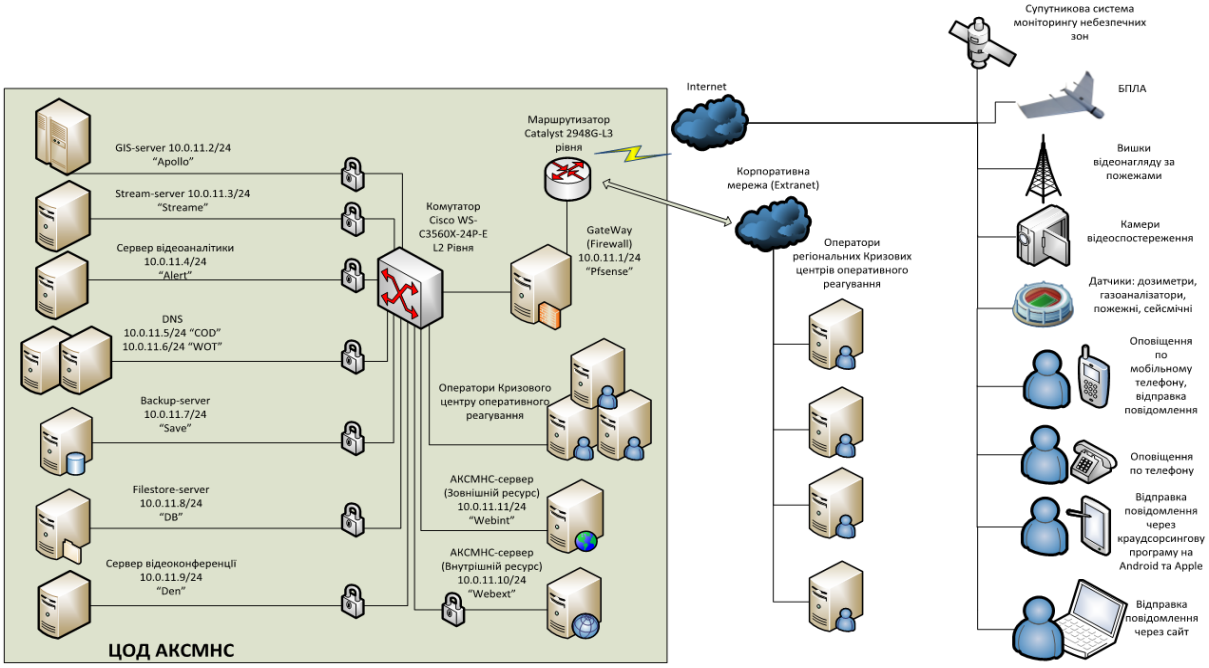


Рис. 1. Структурно-функціональна схема системи

Єдиним середовищем надійної передачі даних може бути безпроводова радіомережа. Задля уникнення взаємних завад треба орієнтуватися на регіональні стандарти, серед яких слід виділити LoRaWAN. Це протокол рівня передачі даних, розроблений компанією LoRa Alliance у 2015 році, для забезпечення рішення з'єднання з низьким енергоспоживанням для кінечних пристроїв, які працюють від акумуляторів [8]. Поточна специфікація LoRaWAN становить 1,1 [9], а найбільш використовувана специфікація - 1,0,3 [10]. Фізичний рівень, що використовується протоколом LoRaWAN, називається LoRa. Він був розроблений компанією Semtech і заснований на модуляції Chirp Spread Spectrum (CSS). Модуляція CSS використовує коефіцієнт розповсюдження (SF) для розповсюдження інформації по частоті. SF є ортогональними один до одного і визначають кількість звукових сигналів на символ сигналу.

У мережах LoRa існує шість можливих SF, від 7 до 12, що визначають кількість бітів, необхідних для передачі однакової кількості даних. Більша кількість бітів на символ збільшує здатність приймача демодулювати повідомлення. Більший SF означає, що для надсилання тієї ж інформації потрібно більше бітів. Однак можна розгорнути кінцевий пристрій далі від шлюзу. Ортогональність між SF забезпечує гарантію, що різні кінцеві пристрої можуть передавати свої пакети з однаковою частотою, але з використанням різних SF. Доступні три смуги пропускання: 125, 250 та 500 кГц. Зазвичай мережі використовують смугу пропускання 125 кГц.

Співвідношення між SF, пропускною здатністю та розміром пакета є важливим для визначення часу в ефірі (ToA), тобто загального часу, коли одна передача використовує повітряний інтерфейс для відправки пакету. Два пакети з однаковим розміром, що використовують однакову пропускну здатність, але з різним SF, мають абсолютно різні ToA.

Для порівняння: для передачі пакету на 50 байт із використанням смуги пропускання 125 кГц ToA становить 0,113 с для SF 7, тоді як при використанні SF 12 ToA становить 2,62 с. Враховуючи лише ToA, затримка доставки пакету принаймні в 20 разів вища при SF 12, ніж SF 7. Більш детальне порівняння, включаючи інші SF, знаходиться в [9]. Вибраний SF, пропускна здатність та розмір пакету безпосередньо впливають на пропускну здатність посилання. Пристрій, що передає з низьким значенням SF, має більшу пропускну здатність, ніж пристрій, що передає з високим значенням SF. Однак збільшення SF також збільшує дальність передачі. У таблиці 1 узагальнено зв'язок між SF, пропускною здатністю та ToA, враховуючи пакети з різними розмірами корисного навантаження, смугою пропускання 125 кГц та без обмежень робочого циклу.

LoRa використовує промислові, наукові та медичні частоти (ISM), і кожна країна чи регіон має свій діапазон частот. Європа використовує 868 МГц, тоді як США, Бразилія та Австралія використовують 915 МГц.

Кожна країна також використовує схему частот піддіапазонів для створення каналів передачі даних. Кожен піддіапазон складається з ряду частот, що називаються каналами.

Таблиця 1. Швидкість та час передачі пакетів

50 байт пакет				Максимальна довжина пакету	
SF	ToA (s)	Швидкість (bits/s)	Payload	Max ToA (s)	Швидкість (bits/s)
7	0.113	3543.1	242	0.394	4913.7
8	0.205	1948.2	242	0.697	2777.6
9	0.369	1082.1	115	0.677	1358.9
10	0.698	572.8	51	0.698	584.5
11	1.478	270.5	51	1.479	275.9
12	2.629	152.1	51	2.793	146.1

Наприклад, Австралія використовує піддіапазони, які складаються з восьми каналів (частот), що використовують смугу пропускання 125 кГц. Піддіапазон необхідний для розділення мереж в одній області за допомогою різних частот.

На рис. 2 представлена схема каналів для Європи (EU868), США (US915) та Австралії (AU915).

Європейський регламент визначає, що канали мережі можуть бути вільно атрибутовані. Однак усі кінцеві пристрої повинні реалізовувати три канали за замовчуванням (868,1 МГц, 868,3 МГц і 868,5 МГц). Сполучені Штати та Австралія мають подібну схему каналів з 64 каналами висхідної лінії зв'язку, які використовують смугу пропускання 125 кГц та лінійно збільшуються на 200 кГц. Обидва регіони також реалізують вісім каналів з пропускною здатністю 500 кГц і лінійно збільшуються на 1,6 МГц. Різниця між US915 і AU915 полягає в каналі низхідної лінії зв'язку. Обидва канали мають вісім каналів, що використовують смугу пропускання 500 кГц, але US915 використовує відокремлену смугу від схеми висхідної лінії зв'язку, тоді як в AU915 низхідна лінія перекриває частоти висхідної лінії зв'язку. Країни та регіони також можуть визначити, скільки часу один пристрій може використовувати канал, застосовуючи обмеження робочого циклу. У Європі робочий цикл становить 1%.

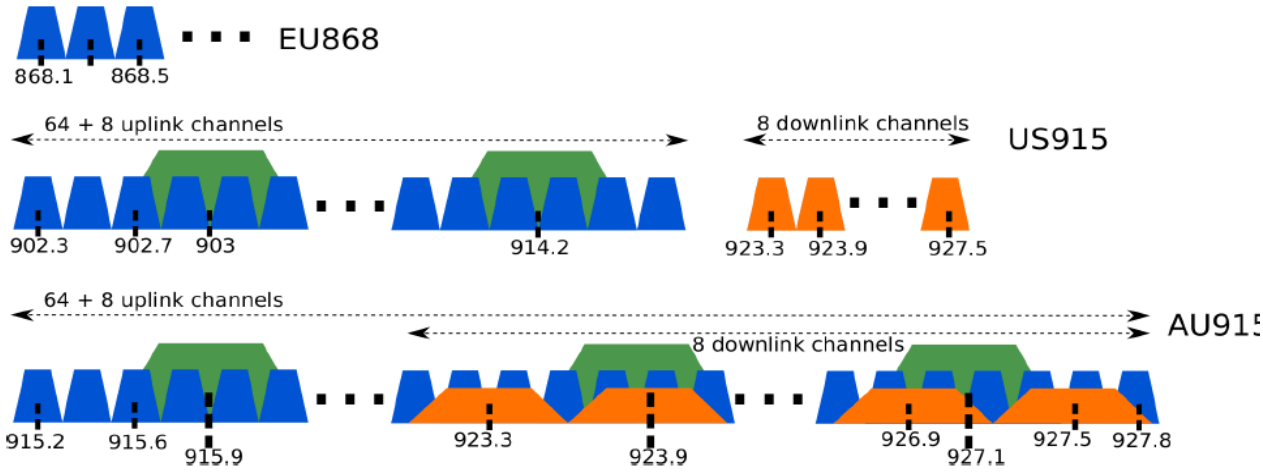
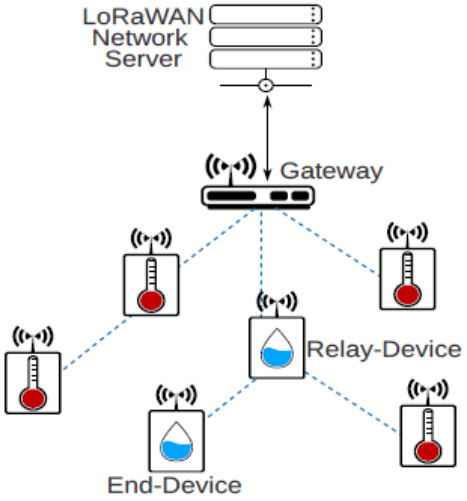


Рис. 2. Легальні регіональні діапазони для LoRa

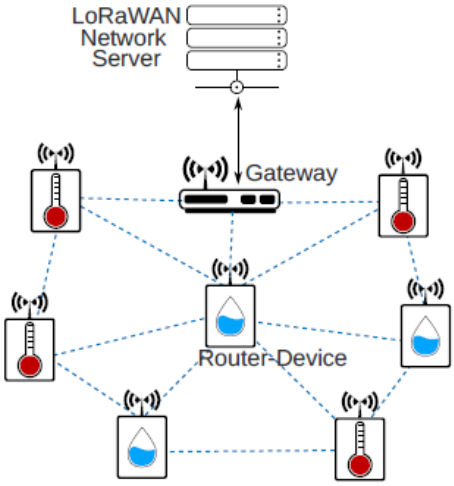
Для забезпечення або поліпшення з'єднання віддалених вузлів можна використовувати ретрансляційні пристрої. На рис. 3a представлено рішення з використанням пристроїв ретрансляції, де пристрій ретрансляції також працює як звичайний кінцевий пристрій. Рішення підходить для розумного будинку або промислового застосування, де є кінцеві пристрої наприклад, доступ до джерела живлення. На рис. 3b показано рішення реле з релейними шлюзами. Однією з важливих відмінностей рішення Relay-Device порівняно з Relay-Gateway є те, що Relay-Device може бути від батареї чи ні, тоді як Relay-Gateway повинен бути обмежений енергією. Relay-Gateway використовує багатоканальну радіостанцію, що дозволяє пристрою слухати принаймні вісім частот, що дозволяє Relay-Gateway концентрувати трафік з віддалених кінцевих пристроїв без будь-якого механізму для вибору частоти, що використовується. Сільський сценарій дуже підходить для використання релейного шлюзу для підключення віддалених пристроїв до головного шлюзу.

На рис. 3c представлена архітектура, що складається з пристроїв ретрансляції та шлюзів ретрансляції. Прикладом сценарію змішаної ретрансляційної мережі є розумне місто, де існує необхідність підключати віддалені пристрої та концентрувати трафік у різних точках мережі.

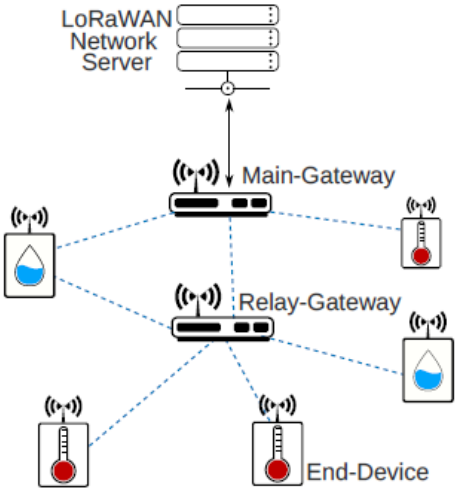
Пристрій ретрансляції може забезпечити підключення до віддаленого кінцевого пристрою, а шлюз ретрансляції може агрегувати дані з набору кінцевих пристроїв (і пристроїв ретрансляції) для доставки своїх повідомлень до головного шлюзу.



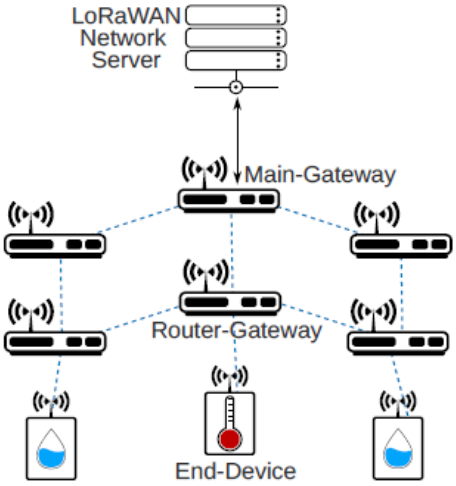
(a) Relay-Devices



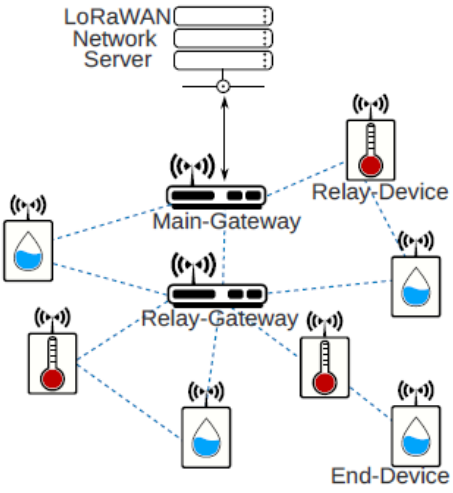
(a) Router-Devices



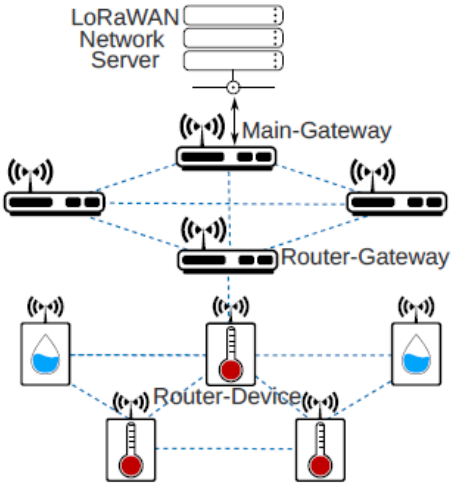
(b) Relay-Gateway



(b) Router-Gateway



(c) Relay-Device and gateway



(c) Router-Device and gateway

Рис. 3. Топологія з вузлами-ретрансляторами

Рис. 4. Топологія з вузлами-маршрутизаторами

Топологія маршрутизатора описує мережеві архітектури на основі пристроїв з можливостями маршрутизації. Протоколи маршрутизації можуть працювати на кінцевих пристроях або на рівні шлюзу.Рис. 4a, b зображують обидва рішення окремо, а рис. 3c розміщує в одній і тій же інфраструктурі два рівні маршрутизації. Рис. 3a може представляти такий сценарій, як розумний будинок з великою кількістю вузлів у складній мережі з доступом до джерела живлення та з великою кількістю бар'єрів передачі.

Оскільки кінцеві пристрої мають меншу вартість у порівнянні з апаратним забезпеченням шлюзу, можна допустити використання маршрутизаторів для цього сценарію.

На рис. 4б представлені кінцеві пристрої, підключені лише до одного маршрутизатора-шлюзу. Однак можна визнати, що кінцевий пристрій може мати з'єднання з декількома маршрутизаторами-шлюзами одночасно. У цьому випадку маршрутизаторам-шлюзам доведеться управляти продубльованими пакетами в мережі, щоб уникнути зайвого трафіку даних. Ферма з деякими пунктами енергетичної інфраструктури, така як центральний зрошувальний стрижень, дуже підходить для використання рішення Router-Gateway. Кожен маршрутизатор-шлюз може працювати як концентратор пакетів деяких кінцевих пристроїв і визначати кращий шлях для пересилання інформації через головний шлюз. Важливо також визнати, що у кожного маршрутизатора-шлюзу може бути відключене підключення до іншої мережі, наприклад 4G або 5G, доки менеджер мережі не вирішить його ввімкнути.

На рис. 4в показано взаємозв'язок між різними рівнями маршрутизації, одним для пристроїв маршрутизатора, а іншим - маршрутизаторами. Протокол маршрутизації, менеджер мережі та фізичні обмеження визначать, чи буде один або кілька пристроїв маршрутизатора підключені до одного або декількох шлюзів маршрутизатора. Сценарій важливий для забезпечення надійного з'єднання з віддаленими або обмеженими зонами, такими як підземне розгортання, з додаванням рівня шлюзу маршрутизації.

Також можлива реалізація гібридної топології, де частина мережі використовує маршрутизатори, а інша частина використовує реле, ретранслятори. І рівень маршрутизації, і рівень ретрансляції можуть бути реалізовані на рівні кінцевих пристроїв або на рівні шлюзу. Кілька кінцевих пристроїв могли передавати пакети даних на пристрій ретрансляції, а пристрій ретрансляції пересилає всі дані на шлюз маршрутизатора. Нарешті, маршрутизатор-шлюз буде відправляти всі пакети, поки вони не досягнуть головного шлюзу. Інший варіант - це підмережа, сформована маршрутизаторами-пристроями, підключеними до одного шлюзу ретрансляції, яка буде пересилати повідомлення на головний шлюз. Більшість рішень для ретрансляторів та маршрутизаторів використовують топологію, показану на рис 3a та 4a, відповідно. Жодна з пов'язаних робіт не представляє мережевого рішення, як на рис. 3c та 4c, що використовує пристрої ретрансляції та шлюзи ретрансляції або пристрої маршрутизатора та маршрутизатори відповідно [6].

Висновки Ідея технологічного продукту полягає в інтеграції сучасної інтелектуальної сенсорної техніки (датчики моніторингу радіації, хімічних забруднень і параметрів навколишнього середовища, безпілотні літальні апарати) із сучасними інформаційно-телекомунікаційними технологіями (бездротові сенсорні мережі, геоінформаційні системи й ін.). Моніторингові датчики повітряного, наземного й водного базування через мережу радіозв'язку забезпечують оперативний дистанційний моніторинг зони спостереження потенційно-небезпечних об'єктів, а геоінформаційні технології забезпечують візуалізацію й 3D географічну прив'язку отриманої інформації до конкретного потенційно небезпечного об'єкту.

Технологія становить значний інтерес для служб моніторингу потенційно небезпечних техногенних об'єктів, оскільки дозволяє вберегти персонал від ураження небезпечними фізико-хімічними й біологічними уражаючими факторами, спрощує процедуру й підвищує оперативність збору інформації про стан навколишнього середовища й підвищує швидкість ухвалення рішення під час позаштатних ситуацій.

Запропонована технологія вирішує проблему ринку моніторингових і інформаційно-телекомунікаційних технологій в галузі атомної енергетики, хімічної промисловості, захисту навколишнього середовища й здоров'я людей.

Цільовими клієнтами є об’єкти критичної інфраструктури, наприклад атомні електростанції, регіональні сховища радіоактивних відходів, небезпечні хімічні виробництва й інші потенційно-небезпечні об'єкти, а саме служби, що займаються моніторингом радіаційної й хімічної обстановки, наприклад, лабораторії автоматизованої системи контролю радіаційної обстановки (АСКРО) на українські й закордонних АЕС тощо.

Були проведені попередні консультації із представниками атомних електростанцій щодо можливості впровадження запропонованої технології в рамках системи АСКРО або як доповнення до неї у випадку надзвичайної ситуації.

Один із способів виявлення уражаючих чинників НС, що загрожують життю людей, таких ознак - аналіз інформації, отриманої з різних джерел за допомогою технічних засобів, а саме: датчиків (дозиметрів, газових датчиків, датчиків землетрусів, димових датчиків, теплових датчиків), безпровідних сенсорних мереж, відеореєстраторів, мобільних пристроїв (відправлення SMS, запис відео і фотографування з місця виникнення НС за допомогою прикладних програм).

Література

1. Зелена книга з питань захисту критичної інфраструктури в Україні: зб. матеріалів міжнар. експерт. нарад / Упоряд. Д.С. Бірюков, С.І Кондратов, за заг. ред. О.М. Суходолі. – К. : НІСД, 2016. – 176 с.

2. On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection: Council Directive 2008/114/EC [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu.

3. Чумаченко С.М. Оцінювання загроз об'єктам критичної інфраструктури / С. М. Чумаченко, В.В. Троцько // Науковий вісник: Цивільний захист та пожежна безпека– Вип. 1 (3). – К.: УкрНДІ ЦЗ, 2017. – С. 41-47

4. Чумаченко С.Н. Оценка риска возникновения пожаров на торфяниках Киевской области и выработка путей его снижения // Сборник научных трудов VII Международной научно-практической конференци "Чрезвычайные ситуации: предупреждение и ликвидация" (Минск, 1 ноября 2016 г.) В 2-х частях. /С.Н. Чумаченко, В.В.Троцько/ Том. Часть 1, 2016. С. 29-39

5. Чумаченко С.М. Концепція автоматизованої краудсорсингової системи моніторингу надзвичайних ситуацій на об'єктах критичної інфраструктури міста / С.М. Чумаченко, С.В. Валуйський, О.М. Тесленко, О.І. Лисенко // Науковий вісник Академії муніципального управління. Серія : Техніка. - 2014. - Вип. 2. - С. 157-163. - Режим доступу: http://nbuv.gov.ua/UJRN/Nvamu_teh_2014_2_20.

6. Михайлова А. В., Чумаченко С. М., Мошенський А. О., Кірієнко М. М. Моделювання мережі NVIS зв`язку для оповіщення про загрозу або виникнення надзвичайної ситуації в агропромисловому комплексі на сході України. Інженерія природокористування. 2019. № 4(14). С. 114-121.

7. LoRaWAN Mesh Networks: A Review and Classification of Multihop Communication Jeferson Rodrigues Cotrim * and João Henrique Kleinschmidt. Available online: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7435450/pdf/sensors-20-04273.pdf (accessed on 30 Dec 2020)

8. LoRa Alliance. LoRaWANTM 1.0 Specification. 2015. Available online: https://lora-alliance.org/resourcehub/lorawanr-specification-v10 (accessed on 30 Dec 2020)

9. LoRa Alliance. LoRaWANTM 1.1 Specification. 2017. Available online: https://lora-alliance.org/resourcehub/lorawanr-specification-v11 (accessed on 30 Dec 2020)

10. LoRa Alliance. LoRaWANTM 1.0.3 Specification. 2018. Available online: https://lora-alliance.org/resourcehub/lorawanr-specification-v103 (accessed on 30 Dec 2020)

References

1. Zelena knyha z pytan zakhystu krytychnoi infrastruktury v Ukraini: zb. materialiv mizhnar. ekspert. narad / Uporiad. D.S. Biriukov, S.I Kondratov, za zah. red. O.M. Sukhodoli. – K. : NISD, 2016. – 176 p.

2. On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection: Council Directive 2008/114/EC [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu.

3. Chumachenko S.M. Otsiniuvannia zahroz ob'iektam krytychnoi infrastruktury / S. M. Chumachenko, V.V. Trotsko // Naukovyi visnyk: Tsyvilnyi zakhyst ta pozhezhna bezpeka– Vyp. 1 (3). – K.: UkrNDI TsZ, 2017. – P. 41-47.

4. Chumachenko S.N. Ocenka riska vozniknovenija pozharov na torfjanikah Kievskoj oblasti i vyrabotka putej ego snizhenija // Sbornik nauchnyh trudov VII Mezhdunarodnoj nauchno-prakticheskoj konferenci "Chrezvychajnye situacii: preduprezhdenie i likvidacija" (Minsk, 1 nojabrja 2016 g.) V 2-h chastjah. /S.N. Chumachenko, V.V.Troc'ko/ Tom. Chast' 1, 2016. P. 29-39.

5. Chumachenko S.M. Kontseptsiia avtomatyzovanoi kraudsorsynhovoi systemy monitorynhu nadzvychainykh sytuatsii na ob'iektakh krytychnoi infrastruktury mista / S.M. Chumachenko, S.V. Valuiskyi, O.M. Teslenko, O.I. Lysenko // Naukovyi visnyk Akademii munitsypalnoho upravlinnia. Seriia : Tekhnika. - 2014. - Vyp. 2. - P. 157-163. - Rezhym dostupu: http://nbuv.gov.ua/UJRN/Nvamu_teh_2014_2_20.

6. Mykhailova A.V., Chumachenko S.M., Moshenskyi A.O., Kiriienko M.M. Modeliuvannia merezhi NVIS zv`iazku dlia opovishchennia pro zahrozu abo vynyknennia nadzvychainoi sytuatsii v ahropromyslovomu kompleksi na skhodi Ukrainy. Inzheneriia pryrodokorystuvannia. 2019. № 4(14). P. 114-121.

7. LoRaWAN Mesh Networks: A Review and Classification of Multihop Communication Jeferson Rodrigues Cotrim * and João Henrique Kleinschmidt. Available online: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7435450/pdf/sensors-20-04273.pdf (accessed on 30 Dec 2020).

8. LoRa Alliance. LoRaWANTM 1.0 Specification. 2015. Available online: https://lora-alliance.org/resourcehub/lorawanr-specification-v10 (accessed on 30 Dec 2020)..

9. LoRa Alliance. LoRaWANTM 1.1 Specification. 2017. Available online: https://lora-alliance.org/resourcehub/lorawanr-specification-v11 (accessed on 30 Dec 2020).

10. LoRa Alliance. LoRaWANTM 1.0.3 Specification. 2018. Available online: https://lora-alliance.org/resourcehub/lorawanr-specification-v103 (accessed on 30 Dec 2020).

Аннотация

Автоматизированная система передачи данных о состоянии объектов критической инфраструктуры с применением современных информационно-телекоммуникационных технологий

С.Н. Чумаченко, А.С. Парталян, А.А. Мошенский, М.Л. Сукало, Л.Д. Филатова

В статье приведены результаты исследования авторов по применению современных информационно-телекоммуникационных технологий для передачи мониторинговой информации о состоянии объектов критической инфраструктуры. На сегодняшний день эти объекты являются ключевыми для работы систем жизнеобеспечения страны и поддержания на должном уровне техногенной и кибербезопасности существующей инфраструктуры. Большое значение в условиях роста техногенных аварий и катастроф уделяется разработке современных подходов для системы предупреждения и мониторинга чрезвычайных ситуаций на потенциально опасных объектах критической инфраструктуры. Значительные усилия сосредотачиваются на создании реальных технических решений построения беспроводных сенсорных сетей с использованием интеллектуальных мониторингово-сигнальных датчиков, беспилотных летательных аппаратов и геоинформационных технологий для обеспечения оперативного мониторинга таких объектов и прилегающих территорий.

Одной из ключевых компонент такой технологии является телекоммуникационная, основанная на новых подходах к реконфигурации радиосетей. Средой надежной передачи данных о состоянии объектов критической инфраструктуры может быть беспроводная радиосеть, которая будет функционировать в сложных условиях чрезвычайных ситуаций. Учитывая значительную насыщенность радиопространства во избежание взаимных помех надо ориентироваться на региональные стандарты, среди которых следует выделить LoRaWAN, разработанный компанией LoRa Alliance в 2015 году для обеспечения соединения с низким энергопотреблением для конечных устройств, работающих от аккумуляторов.

В статье детализированы протоколы стандарта LoRaWAN и ключевые подходы к разработке различных топологий таких радиосетей для регионов Европы, США и Австралии. Проведен анализ топологий беспроводных сенсорных сетей и их прикладного применения для создания различных радиосетей. Целевыми клиентами таких радиосетей являются объекты критической инфраструктуры, например атомные электростанции, региональные хранилища радиоактивных отходов, опасные химические производства и другие потенциально опасные объекты, и службы ГСЧС, занимающихся мониторингом радиационной и химической обстановки.

Ключевые слова: *критическая инфраструктура, диапазон частот, ретрансляция, маршрутизатор, пропускная способность.*

Abstract

Automated system of transmission of data on the state of critical infrastructure objects with the use of modern information and telecommunications

S.M. Chumachenko, A.S. Partalian, A.A. Moshensky, M.L. Sukalo, L.D. Filatova

The article presents the results of the authors' research on the use of modern information and telecommunication technologies for the transmission of monitoring information about the state of critical infrastructure. Today, these facilities are key to the operation of the country's life support systems and support at the appropriate level of man-made and cybersecurity of existing infrastructure. In the context of the growth of man-made accidents and catastrophes, great importance is attached to the development of modern approaches to the system of prevention and monitoring of emergencies at potentially dangerous critical infrastructure. Significant efforts are focused on creating realistic technical solutions for the construction of wireless sensor networks using intelligent monitoring and signaling sensors, unmanned aerial vehicles and geographic information technologies to ensure operational monitoring of such facilities and surrounding areas.

One of the key components of such technology is telecommunications, which is based on new approaches to the reconfiguration of radio networks. A wireless radio network that can operate in complex emergencies can be a medium for the reliable transmission of critical infrastructure data. Given the significant saturation of

the radio space, regional standards should be considered to avoid mutual interference, including LoRaWAN, developed by LoRa Alliance in 2015 to provide a low-power connection for battery-powered end devices.

The article details the protocols of the LoRaWAN standard and key approaches to the development of different topologies of such radio networks for the regions of Europe, the USA and Australia. The analysis of topologies of wireless sensor networks and their application for creation of various radio networks is carried out. The target customers of such radio networks are critical infrastructure facilities, such as nuclear power plants, regional radioactive waste repositories, hazardous chemical plants and other potentially hazardous facilities, and SES services that monitor radiation and chemical conditions, etc.

Keywords*: critical infrastructure, frequency range, relay, router, bandwidth.*

Бібліографічне посилання/ Bibliography citation: Harvard
Chumachenko, S. M. et al. (2021) “Automated system of transmission of data on the state of critical infrastructure objects with the use of modern information and telecommunications,” *Engineering of nature management*, (3(21), pp. 127 - 135.

Подано до редакції / Received: 26.04.2021