ЕЛЕКТРОМЕХАНІКА, ЕЛЕКТРОТЕХНІКА ТА ЕНЕРГЕТИКА

DOI 10.31891/2307-5732-2020-287-4-143-148
УДК 621

К.Л. ГОРЯЩЕНКО, А.А. ТАРАНЧУК, Я.В. СУПРУНЮК
Хмельницький національний університет
О.В. ЦИРА
Одеська національна академія зв'язку ім. О.С. Попова

ЗАСТОСУВАННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ В СИСТЕМАХ ОБМЕЖЕНОЇ ПРОЦЕСОРНОЇ ПОТУЖНОСТІ

Один з напрямків розвитку безпроводових систем передачі інформації ґрунтується на впровадженні мереж на базі простих вузлів, що використовуються в таких стандартах, як ZigBee, Bluetooth, Wibree. Інформація, що передається мережею, може бути перехоплена та використана третьою стороною. Простота конструкції, мінімальне енергоспоживання та мінімальний обсяг пам'яті не дозволяють впровадити складні алгоритми криптографічного захисту інформації. Складність алгоритму захисту обумовлена розрядністю процесора (8, 16 або 32 біти), наявним обсягом пам'яті ПЗП та ОЗП, а також енергоспоживанням в процесі виконання криптографічного перетворення. Обсяг пам'яті також є важливим для прийняття, обробки та передачі інформації між вузлами мережі.

Ключові слова: безпроводова мережа, вузол, криптографія.

K.L. HORIASHCHENKO, A.A. TARANCHUK, Y.V. SUPRONYUK
Khmelnitsky national university, Ukraine
O. TSYRA
Odessa national academy of communication named by O. Popov

APPLICATION OF CRYPTOGRAPHIC ALGORITHMS IN SYSTEMS WITH LIMITED PROCESSING POWER

One of the directions of development of wireless information transmission systems is based on the introduction of networks based on simple nodes used in such standards as ZigBee, Bluetooth, Wibree. Information transmitted over the network may be intercepted and used by a third party. Simplicity of design, minimum power consumption and minimum amount of memory do not allow to implement complex algorithms of cryptographic protection of information. The complexity of the protection algorithm is due to the bit size of the processor (8, 16 or 32 bits), the available amount of RAM and RAM, as well as power consumption during cryptographic conversion. The amount of memory is also important for receiving, processing and transmitting information between network nodes.

One of the possible ways to increase the efficiency of cryptographic operations in hardware is to build them on the principle of "master - slave". The method involves the use of a general-purpose processor as the central head of the device module ("master"), and a specialized arithmetic coprocessor ("master"), which performs all time-consuming operations under the control of the master.

Keywords: wireless network, node, cryptography.

Вступ

Сьогодні у світовій практиці послуг у сфері контролю стану розподілених в просторі вузлів визначилася стійка тенденція на посилення ролі технічних засобів. Тенденція ця не випадкова: численні дослідження в області особистої і майнової безпеки показали, що широке використання технічних засобів дозволяє виключити або звести до мінімуму негативний вплив самої ненадійної ланки в системі - людини, якій властиві стомлюваність, неуважність, халатність і т. п. При цьому, організація розподіленої мережі контролю і передачі за допомогою технічних засобів обходиться споживачеві значно дешевше, а надійність її вища [1, 5].

По факту, в середині 90-х років, такими вузлами мережі контролю і передачі ставали системи безпеки для охоронних систем.

У завданнях 2020-х років - розподілені системи контролю за станом здоров'я людей в приміщеннях, на вулиці, в транспорті і так далі. Глобальна пандемія вірусу COVID - 19 веде до усвідомленої необхідності створення медичних мереж контролю.

Історично, при створенні систем розподіленого контролю основна увага приділялася таким аспектам, як [1]:

- автоматизація, яка дозволяє до мінімуму спростити процеси введення об'єктів під охорону, скоротити обслуговуючий персонал; істотно скоротити кількість неправдивих тривог через втручання в роботу системи;
- контроль каналу зв'язку, що забезпечує високу достовірність передачі і виключає втрату тривожної інформації;
- розробка широкої гамми об'єктових пристроїв з різними функціональними і сервісними можливостями, що дозволяють задовольнити потреби найширших верств населення.

З точки зору організації захисту об'єктів від несанкціонованого проникнення, як по устаткуванню технічними засобами охорони, так і по тактиці дій чергових служб, існуючі системи не мають яких-небудь істотних відмінностей.

Передача інформації з використанням безпроводових технологій

Питання про достовірне та безпечне надсилання інформації від приймача до отримувача відоме ще з давніх часів. Основним завданням криптографії в давні часи було забезпечення конфіденційності, або простіше кажучи шифрування – інформація, що містилася, мала бути змінена таким чином, щоб прочитати та зрозуміти міг лише той, кому дійсно назначено [1], а не будь-яка інша стороння особа, без відомостей про спосіб, яким було зашифрована відповідна інформація.

Криптографічним алгоритмом (шифром) називається така математична функція, що дозволяє виконати над інформацією дію шифрування та дешифрування.

Найпопулярнішим способом в давні часи був так званий шифр Цезаря (або інша назва – шифр зсуву) – шифрування інформації, що передавалася на папері, в якому кожна буква тексту, що був написаний, замінювалась на ту, яка була віддалена (зсунута) на три позиції в буквенному алфавіті. Простий для нинішньої техніки шифр, став основою для складніших способів, до прикладу шифр Віженера чи ROT13 [1, 1, 6].

З розвитком людства і науки, такі способи шифрування інформації ставали все більш неефективними. Наступним кроком стали машини, які виконували шифрування та дешифрування інформації, найвідомішою з яких є Енігма. Та з появою комп'ютерних систем, можна було зашифрувати будь-які дані, представивши їх у двійковому вигляді, а не лише у текстовому вигляді, як це відбувалося доволі довгий період людства.

В наш час це питання так і залишилось актуальним, тільки тепер інформацією обмінюються не лише люди, а й пристрої, які оточують нас. І чим більше є таких пристроїв, тим гостріше стає це питання.

Перед криптографічними методами завжди висувають наступні вимоги [4]:

1. Зашифроване повідомлення можливо прочитати лише при наявності ключа.

2. Кількість операцій, що потрібні для визначення використаного ключа шифрування по фрагменту зашифрованого повідомлення й відповідного відкритого тексту, повинно бути не менше загального числа можливих ключів.

3. Кількість операцій, які необхідні для розшифрування повідомлення способом перебору ключів, повинно мати строгу нижню порогову оцінку й виходити за межі можливостей сучасного обладнання, або вимагати високі витрати на обчислення.

4. На надійність захисту шифрованої інформації не впливає знання сторонніми алгоритму шифрування.

5. Маленька зміна ключа шифрування призводить до істотних змін самої зашифрованої інформації, навіть при шифруванні вихідного тексту, який був зашифрований.

6. Незначна зміна вихідного тексу призводить до істотних змін зашифрованої інформації, при використанні того ж ключа шифрування.

7. Структурні елементи алгоритму шифрування завжди залишаються без змін.

8. Додаткові біти, що вводяться в інформацію, в процесі її шифрування, повинні бути надійно сховані в зашифрованій інформації.

9. Довжина зашифрованої інформації не повинна перевищувати загальну довжину вихідної інформації.

10. Мають бути виключені прості та легкі залежності, які використовуються для формування ключа шифрування.

11. Будь-який ключ з множини ключів має забезпечувати надійний захист інформації.

12. Реалізація алгоритму повинна бути як на програмному та апаратному рівні.

Тому в цілях подальшого розвитку і вдосконалення систем збору та передачі інформації до нових розробок останнім часом пред'являються додаткові вимоги:

- імітостійкість і криптозахист, системи, що забезпечують стійкість, до несанкціонованого «обходу» і обумовлені появою «кваліфікованих» крадіжок;
- висока інформативність, що забезпечує розділення сигналів про проникнення і пожежу, аварію або зміну параметрів лінії зв'язку і т. д.;
- можливість сполучення системи з оптоволоконними каналами зв'язку, обумовлена впровадженням підприємствами зв'язку нових цифрових технологій передачі інформації;
- уніфікація створюваних технічних засобів, тобто можливість об'єднання різних пристроїв в єдиний програмно-апаратний комплекс збору та передачі інформації.

Пріоритетним завданням технічної політики в області розвитку таких систем є розробка відсутніх на сьогодні єдиних вимог, що в умовах різноманіття існуючих і нових, дозволить уніфікувати стики систем передачі сповіщень.

Передача інформації з використанням бездротових технологій

Разом з ростом технологій та розвитком мобільних пристроїв, стало зрозуміло, що дріт використовувати можна на невеликих відстанях, і для пристроїв, що в більшості випадків використовуються стаціонарно, без переміщення по великих площах. Постало питання про впровадження бездротового з'єднання, для передачі інформації між пристроями на відкритій місцевості. Таким чином, почався розвиток бездротового підключення. В залежності від відстані, на якій буде передаватись інформація, бездротові мережі можна поділити на три класи: WPA, WLAN, WMAN.

За дальністю дії, бездротові мережі, можна поділити наступним чином [7]:

WPAN – бездротова мережа, що охоплює невелику частину території, невелику швидкість передачі інформації, а також передача інформації відбувається лише між декількома пристроями. Прикладом такої технології є Bluetooth, ZigBee.

WLAN – бездротова мережа, що охоплює середню за розміром ділянку (відстанню до 100 метрів), в залежності від використання стандарту передачі та частоти розміщення, швидкість передачі може сягати до 3,4 Гбіт/с. Прикладом такої технології є Wi-Fi.

WMAN – бездротова мережа, що охоплює велику територію (область покриття до 50 кілометрів). В залежності від використання стандарту, швидкість передачі може варіюватись, максимальним значенням є 1 Гбіт/с. Прикладом такої технології є WiMax.

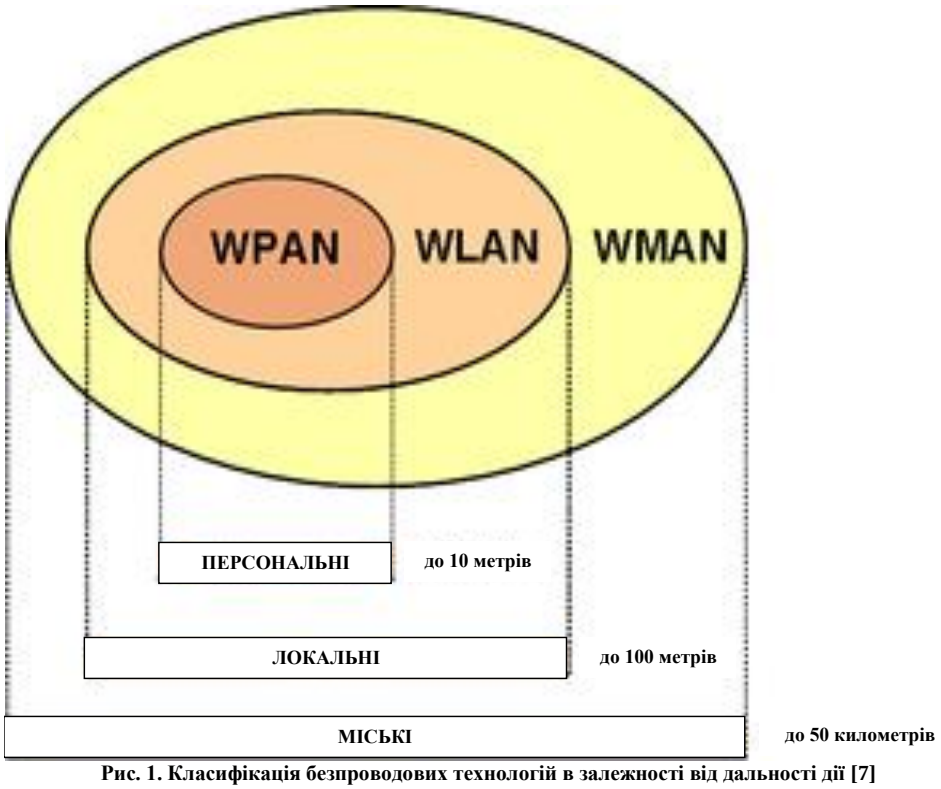

Рис. 1. Класифікація безпроводових технологій в залежності від дальності дії [7]

Безпровідні сенсорні мережі - це розподілені мережі, що мають здатність до реорганізації власної структури. Характеризуються стійкістю до відмови окремих елементів цієї мережі, а також обмінюються інформацією по безпровідному зв'язку. Кожен елемент мережі має автономне джерело живлення, мікрокомп'ютер, приймач/передавач.

Виділяють наступні основні стандарти для малопотужних безпровідних мереж:

- IEEE 802.15.4;
- ZigBee;
- Bluetooth;
- Wibree.

Область покриття мережі може складати від декількох метрів до декількох кілометрів, залежно від типу модуля і антени, а також за рахунок здатності ретрансляції повідомлень від одного елементу до іншого. Обмін даними між двома кінцевими пристроями може здійснюватися через ретранслятор, у тому випадку, якщо дальність роботи цих пристроїв не дозволяє їх взаємне виявлення. Таким чином, пристрою з малим радіусом дії за допомогою системи ретрансляторів можуть спілкуватися один з одним.

Постановка проблеми дослідження на прикладі пристроїв мережі ZigBee

Пристрої безпроводової системи забезпечують можливість швидкого створення мережі. Як було показано вище, пристрої володіють власним джерелом живлення. Це джерело часто є простою батареєю з невеликою ємністю та призначеною для одноразового використання. Сам датчик-вузел мережі не підлягає ремонту або заміні в процесі експлуатації. Основна причина такого ставлення – відносна простота конструкції, мінімальний розмір та низька ціна. Наприклад, на рис. 2 наведено приклад включення модуля ZigBee (тип RC2300) для обміну даними по послідовному порту. Як видно з рисунку, модуль забезпечує функціонал зчитування, обробки, зв’язку та передачі.

У технології ZigBee використовується два типи модулів зв’зку різної складності. Повністю функціональний пристрій (FFD — Full Function Device) здатний приймати і передавати дані, у тому числі і чужі (по ланцюжку). При об'єднанні FFD -устройств можуть бути реалізовані топології «зірка», «кожен з кожним» і «кластерне дерево».

Пристрій з обмеженим набором функції (RFD — Reduced Function Device) — це найпростіший тип, який може тільки переговорюватися з координуючим пристроєм. При об'єднанні в мережу RFD може використовуватися тільки в топології «зірка». Окрім ділення на FFD і RFD в специфікації ZigBee визначені три типи логічних пристроїв — координатор мережі, маршрутизатор і крайовий пристрій.

Координатор ініціалізував мережу, управляє мережевими вузлами, зберігає інформацію про налаштування кожного мережевого вузла, задає номер частотного каналу і ідентифікатор мережі PAN ID.

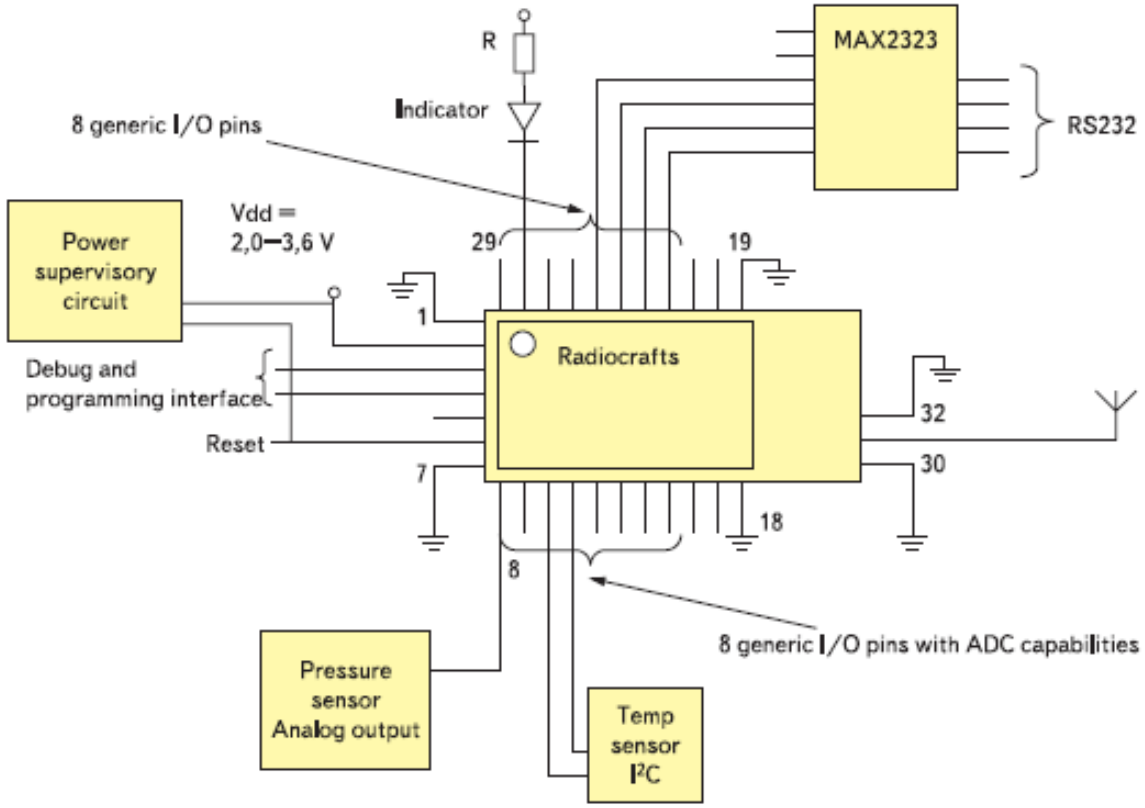

Рис. 2. Приклад включення модуля ZigBee (тип RC2300) для обміну даними по послідовному порту

Проблема апаратної реалізації вузлів розподіленої мережі з підтримкою криптографії

В залежності від пристрою, який використовується кінцевим користувачем, визначається той чи інший клас бездротової передачі інформації.

Взаємодію між відправником і отримувачем з урахуванням криптографічної системи описується наступним чином [1]:

1. Відправник отримує з джерела генерування ключів, ключ К1, яким буде зашифрована інформація – повідомлення М.

2. Відправник зашифровує за допомогою ключа К1 необхідну для передачі інформацію М, та передає криптограму Е відкритими каналами зв'язку в напрямку до одержувача (або одержувачів).

3. Отримувач, за допомогою джерела генерування ключів, отримує необхідний ключ К2, для розшифрування зашифрованої інформації. В залежності від схеми шифрування, ключі К1 та К2 можуть бути однаковими або різними.

4. Отримувач розшифровує за допомогою згенерованого ключа К2 зашифровану інформацію Е, та отримує її в звичайному вигляді для ознайомлення – повідомленні М.

На рис.3 показано також і шифрувальника супротивника. Супротивник намагається досягнути як мінімум дві мети:

1) встановлення ключа розшифрування К2 для можливості зчитування повідомлення М з криптограми Е.

2) встановлення ключа шифрування К1 для можливості зміни повідомлення М або введення в мережу спотворених повідомлень.

3) Отже можна зробити висновок, що криптографічні протоколи, що використовуються в протоколі передачі інформації мають забезпечити надійність від втручення інших сторін не менше певного часу.

Рис. 3. Загальна структурна схема передачі інформації із застосуванням криптографії

Процес розробки апаратних або апаратно-програмних засобів криптографічного захисту інформації на основі сучасних асиметричних криптографічних алгоритмів, у тому числі і національних асиметричних криптографічних алгоритмів [1], безпосередньо пов'язаний з необхідністю реалізації арифметичних операцій, що лежать в основі алгоритмів. Так, стандарт ГОСТ 34.10-2018 використовує числа розмірністю не менше 256 біт, що в десятковому уявленні складає $\approx 10^{77}$:

- великі габарити, що робить неможливим їх застосування в малогабаритних і ношених пристроях, як наприклад в USB - ключах;
- велике споживання електроенергії, що знижує ефективність їх використання в пристроях з батарейним живленням;
- велика кількість виводів : більшість високопродуктивних процесорів мають кількість виводів від 300 і вище, що призводить до небажаних ускладнень схемотехніки проектованих пристроїв. Крім того, конструктивне розташування виводів в сучасних корпусах спричиняє за собою необхідність в дорогому спеціалізованому устаткуванні, що унеможливлює широкий розвиток розробок такого роду (як правило, усі процесори з числом виводів ≥ 200 випускаються в корпусах з кульковими виводами BGA);
- неоптимізована система команд під конкретне завдання: ефективність програмного коду (а значить і швидкість виконання програми) безпосередньо залежить від фіксованої системи команд конкретного процесора;
- обмежена розрядність даних : сучасні процесори мають фіксовану розрядність даних (8, 16 або 32 розряди), що призводить до збільшення програмного коду при виконанні криптографічних операцій, і як наслідок - до зниження продуктивності пристрою в цілому;
- лінійність програмного коду: в процесорах відсутні можливості незалежного і паралельного виконання декількох трудомістких операцій одночасно;
- висока вартість, яка росте пропорційно збільшенню продуктивності.

Висновки

Виходячи з вищенаведеного наведеного, можна зробити висновок, що використання високопродуктивних процесорів для виконання криптографічних операцій в апаратних засобах є малоефективним і недоцільним за рахунок великого енергоспоживання.

Одним із можливих способів підвищення ефективності виконання криптографічних операцій в апаратних засобах є їх побудова за принципом «ведучий - ведений». Спосіб припускає використання процесора загального призначення як центрального керівника модуля пристрою («ведучий»), і спеціалізований арифметичний співпроцесор («ведений»), що виконує усі трудомісткі операції під управлінням ведучого. Це зменшує енергоспоживання в моменти виконання дій прийому інформації та її передачі. Спеціалізований співпроцесор забезпечує швидкість обробки за короткі терміни часу.

Література

1. Горященко К.Л. Формат Adobe PDF как средство распространения защищенной информации / К.Л. Горященко, І.В. Троцишин // Вимірювальна та обчислювальна техніка в технологічних процесах. – Хмельницький. – 2006. – № 1. – С. 132-136.

2. Бабаш А. В. Криптография (аспекты защиты). / А. В. Бабаш, Г. П. Шанкин. — М.: СОЛОН-ПРЕСС, 2007. – 512 с.

3. Панасенко С. П. Аппаратные шифраторы / С. П. Панасенко, В.В. Ракитин // Журнал «Мир ПК». 2002. № 8.

4. Шокало В.М. Концепция создания отечественных специальных цифровых систем передачи информации / В.М. Шокало, А.И. Цопа // Науково-технічний журнал «Захист інформації». – Київ: ДУІКТ,

2006. – Вип. №3. – С. 51-57.

5. Горященко К.Л. Ризики цілісності інформації на переносних носіях інформації / К.Л. Горященко, О.І. Полікаровських, В.Є. Гавронський, Ю.І. Сніжко // Вісник Хмельницького національного університету. – 2008. – № 4. – С. 66-70.

6. Горященко К.Л. Аспекти захисту програмного коду у відкритому апаратному середовищі / К.Л. Горященко // Вісник Хмельницького національного університету. – 2009. – № 2. – С. 208-212

7. Стрельницкий А.Е. Вариант повышения помехозащищенности радиоканала фиксированной связи WiMAX / А.А. Стрельницкий, А.И. Цопа, В.М. Шокало // Труды 8-й Международной научно-практической конференции «Современные информационные технологии» /СИЭТ'2007/. – Одесса, 2007. – С. 173.

References

1. Horiashchenko K.L. Format Adobe PDF kak sredstvo rasprostranenija zashhishhennoj informacii / K.L. Horiashchenko, I.V. Trocishin // Vimirjuvalna ta obchisljuvalna tehnika v tehnologichnih procesah. – Hmelnickij. – 2006. – № 1. – S. 132-136.

2. Panasenko S. P., Rakitin V.V. Apparatnye shifratory // Zhurnal «Mir PK». 2002. № 8.

3. Babash A. V., Shankin G. P. Kriptografija (aspekty zashhity). — M.: SOLON-PRESS, 2007. – 512 s.

4. Shokalo V.M. Koncepcija sozdanija otechestvennyh special'nyh cifrovyh sistem peredachi informacii / V.M. Shokalo, A.I. Copa // Naukovo-tehnichnij zhurnal «Zahist informacii». – Kiïv: DUIKT, 2006. – Vip. №3. – S. 51-57.

5. Horiashchenko K.L. Riski cilisnosti informacii na perenosnih nosijah informacii / K.L. Horiashchenko, O.I. Polikarovskih, V.E. Gavronskij, Ju.I. Snizhko // Visnik Hmelnickogo nacionalnogo universitetu. – 2008. – №4. – S. 66-70.

6. Horiashchenko K.L. Aspekti zahistu programnogo kodu u vidkritomu aparatnomu seredovishhi / K.L. Horiashchenko // Visnik Hmelnickogo nacionalnogo universitetu. – 2009. – №2. – S. 208-212

7. Strelnickij A.E., Copa A.I., Shokalo V.M. Variant povyshenija pomehozashhishhennosti radiokanala fiksirovannoj svjazi WiMAX / // Trudy 8-j Mezhdunarodnoj nauchno-prakticheskoj konferencii «Sovremennye informacionnye tehnologii» /SIJeT'2007/. – Odessa, 2007. – S. 173.

Рецензія/Peer review : 19.10.2020 р. Надрукована/Printed : 06.11.2020 р.