

В. Б. Дудикевич, Г. В. Микитин, А. І. Ребець, Р. І. Банах  
 Національний університет “Львівська політехніка”,  
 кафедра захисту інформації

## СИСТЕМНА МОДЕЛЬ БЕЗПЕКИ БЕЗПРОВІДНИХ ТЕХНОЛОГІЙ ЗВ'ЯЗКУ: ШИФРУВАННЯ ДАНИХ У WIMAX- СИСТЕМАХ

© Дудикевич В. Б., Микитин Г. В., Ребець А. І., Банах Р. І., 2014

На основі концепції “об’єкт – загроза – захист” запропоновано системну модель безпеки технологій безпроводного зв’язку на рівні структури “система – сигнал – канал – тракт” та її метрологічного забезпечення. В межах створеної моделі розроблено алгоритмічно-програмне забезпечення процедури шифрування даних для WIMAX-систем на основі стандарту AES та мови програмування C#.

Ключові слова: концепція “об’єкт – загроза – захист”, безпроводні технології зв’язку, системна модель, структура “система – сигнал – канал – тракт”, метрологічне забезпечення, шифрування даних.

## SYSTEM SECURITY MODEL OF WIRELESS CONNECTION TECHNOLOGIES: DATA ENCRYPTION IN WIMAX- SYSTEMS

© Dudykevych V., Mykytyn G., Rebets A., Banakh R., 2014

The system model of wireless technologies security was proposed on a level of the structure “system – signal – channel – tract” and its metrological support according to the conception “object – threat – defence”. The software of data encryption procedure for WiMAX systems based on AES standart and C# programming language was developed in limits of the created model.

Key words: wireless technologies, a defence, a system model, the structure “system – signal – channel – tract”, metrological support, data encryption.

### Вступ

Інформаційно-комунікаційні технології (ІКТ) є вагомим засобом розвитку Національної програми інформатизації. Серед основних напрямів реалізації концепції технічного захисту інформації в Україні – створення методології синтезу систем багаторівневого захисту інформації, адекватних загрозам її безпеки, зокрема в інформаційно-комунікаційних технологіях. У контексті забезпечення функціональної та інформаційної безпеки ІКТ в межах міжнародного і національного інформаційно-комунікаційного простору актуальним є створення комплексної системи захисту даних у безпроводних комунікаціях і цифрових системах зв’язку, спрямованої на забезпечення безпеки інформації від витoku технічними каналами, несанкціонованих дій та спеціального впливу [1, 2].

### Системна модель безпеки безпроводних технологій зв’язку

Безпека та ефективність функціонування безпроводних ІКТ зумовлена: розвитком технологій захисту цифрового обладнання, сигналів і радіочастотних каналів; наявністю методів і засобів метрологічного забезпечення у цифрових системах зв’язку. Розглянемо напрацювання учених у цих двох взаємопов’язаних напрямках. У контексті вдосконалення методів та засобів захисту даних у технологіях зв’язку в праці проаналізовано шаблони аутентифікації в сучасних комунікаційних системах та мережах [3]. Як розвиток підходів та методології забезпечення цілісності захисту інформації в праці [4] подано модель передавання мовного повідомлення по захищеному

безпроводному каналу зв'язку. Аспекти вирішення проблеми виявлення та ідентифікації атак на інформаційно-комунікаційні системи висвітлено в роботах [5, 6]. Засади функціональної безпеки інформаційно-телекомунікаційних систем розвинено в роботі [7] на рівні методу оцінювання ризиків з урахуванням механізмів захисту інформації.

З метою ефективного функціонування технологій цифрового зв'язку, забезпечення якісного рівня надання послуг та забезпечення захищеності інформації, що циркулює в передавально-приймальних трактах, актуальним і необхідним є сегмент метрологічного забезпечення в цифрових системах безпроводного зв'язку. Досягнення необхідної точності та єдності вимірювань параметрів радіосигналів є одним з найголовніших завдань у напрямі забезпечення достовірності передавання-приймання даних, високої пропускної здатності каналів зв'язку, низької ймовірності похибок. В праці [8] проаналізовано стан метрологічного забезпечення для цифрових комунікацій і систем зв'язку. Для забезпечення цілісності функціональної та інформаційної безпеки ІКТ на апаратно-програмному рівні важливою є системна модель захисту даних [9]. Розглянемо особливості системної моделі на основі дворівневої структури об'єкта захисту (рис. 1).

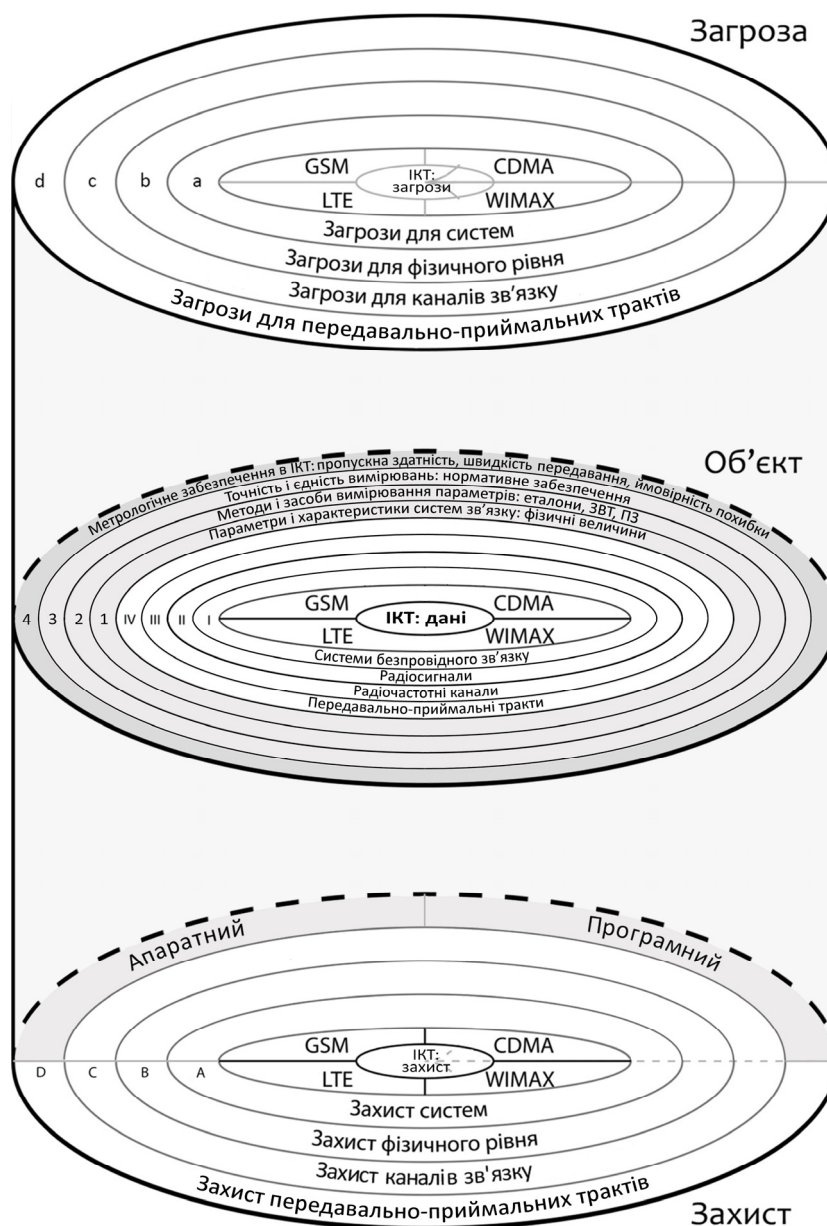


Рис. 1. Системна модель захисту даних у безпроводних технологіях зв'язку

### **Інформаційно-комунікаційні технології зв'язку:**

**GSM** – міжнародний стандарт для цифрового безпроводного зв'язку другого покоління з особливостями функціонування:

- часове та частотне розділення каналів;
- взаємодія трьох підсистем: базових станцій, центру комутації та центру технічного обслуговування;
- використання великої кількості базових станцій, розгорнутих на місцевості.

**CDMA** – одна з технологій множинного доступу з кодовим розділенням каналів, використовується в стандартах цифрового безпроводного зв'язку третього покоління згідно з особливостями функціонування:

- кодове, часове і частотне розділення каналів;
- використання безперервного частотно-часового простору;
- використання множинного доступу на ділянці між базовою станцією та мобільним обладнанням.

**WiMAX** – стандарт безпроводного зв'язку четвертого покоління, який забезпечує широкопasmовий зв'язок на значні відстані й має такі особливості функціонування:

- ортогональне частотне розділення каналів з мультиплексуванням;
- використання з'єднання прямої видимості між базовими станціями;
- взаємодія двох підсистем: мережі доступу і мережі забезпечення послуг.

**LTE** – мобільний стандарт високошвидкісного передавання даних четвертого покоління, що базується на мережевих технологіях GSM/EDGE та UMTS/HSPA. Особливості функціонування:

- ортогональне частотне розділення каналів з мультиплексуванням;
- радіообмін за допомогою циклічних кадрів;
- можливість побудови мережі з використанням технологій попередніх поколінь безпроводного зв'язку.

*Сегмент функціональної та інформаційної безпеки ІКТ на рівні структури “системи – радіосигнали – радіочастотні канали – тракти”:*

- системи (I); радіосигнали (II);
- радіочастотні канали (III); передавально-приймальні тракти (IV).

*Сегмент забезпечення якості передавання-приймання даних на рівні структури “параметри цифрових систем зв'язку – методи і засоби вимірювання параметрів – єдність і точність вимірювань – метрологічне забезпечення”:*

- фізичні величини (1);
- еталони, засоби вимірювальної техніки (ЗВТ), програмне забезпечення (ПЗ) (2);
- система стандартів як нормативна база забезпечення (3);
- висока пропускна здатність, низька імовірність похибки детектування даних (4).

**Рівні об'єкта – структура “система – сигнал – канал – тракт”:**

*Системний рівень (I) (цифрові системи, обладнання):*

- мобільні термінали; базові станції;
- центри комутації; шлюзи і термінали.

*Фізичний рівень (II) (частотні діапазони радіосигналів):*

- GSM: 890 – 960; 1710 – 1880 МГц;
- CDMA: 824 – 849; 869 – 894 МГц; 1920 – 1980, 2110 – 2170 МГц;
- WiMAX: 1,5 – 11 ГГц (до абонента); 10 – 66 ГГц (між станціями);
- LTE: 700 – 2700 МГц (частотна модуляція); 1800 – 3800 МГц (часова модуляція).

*Канальний рівень (III):*

- безпроводні канали зв'язку;
- мідні, волоконно-оптичні кабелі.

*Рівень передавально-приймального тракту (IV) (процедури перетворення):*

- форматування / деформатування;
- шифрування / дешифрування;

- каналне кодування / декодування;
- імпульсна модуляція / демодуляція;
- ущільнення / розуцільнення.

**Рівні загроз структурі “система – сигнал – канал – тракт”:**

*Системний рівень (а):*

- прослуховування мобільних телефонів;
- несанкціонований віддалений доступ до обладнання;
- несанкціонований фізичний доступ до обладнання;
- помилки в адмініструванні / конфігуруванні обладнання;
- атаки на відмову обладнання (DoS / DDoS).

*Фізичний рівень (b):*

- перешкоди під час передавання даних у відповідних частотних діапазонах;
- перехоплення (прослуховування) ефіру;
- модифікація даних у трафіку, що циркулює.

*Канальний рівень (c):*

- несанкціоноване під’єднання пристроїв зчитування інформації;
- вплив сторонніх сигналів, сформованих передавачами на частоті передавального інформаційного сигналу;
- вплив комплексу факторів на інформативні параметри корисного сигналу.

*Рівень передавально-приймального тракту (d) (зовнішній вплив):*

- побічні електромагнітні випромінювання та наведення у контексті перехоплення інформації;
- функціонування поблизу приладів високої напруги як засобів впливу на інформаційний сигнал.

**Рівні захисту структурі “система – сигнал – канал – тракт”**

*Системний рівень (A):*

- вибір телефонів, які перевірені на відсутність пристроїв прослуховування;
- уникнення передавання конфіденційної інформації стільниковим телефоном;
- урахування аспектів складності перехоплення мовного сигналу з рухомого об’єкта;
- обмеження фізичного доступу до обладнання кодовим чи ключовим замком.

*Фізичний рівень (B) (вбудовані алгоритми шифрування даних):*

- GSM – A5/1, A5/2, A5/3;
- CDMA – CAVE;
- WiMAX – DES3, AES;
- LTE – AES, AKA,

*Канальний рівень (C) (модуляція сигналу з частотним і часовим ущільненням):*

- GSM – TDMA, GMSK;
- CDMA – TDMA, FDMA;
- WiMAX – FDD, TDD, OFDM;
- LTE – FDD (OFDM, SC-FDMA), TDD.

*Рівень передавально-приймального тракту (D) (конфіденційність – достовірність – цілісність):*

- апаратне забезпечення безпеки даних в ІКТ: скремблювання та зашумлення;
- програмне забезпечення безпеки даних в ІКТ: алгоритми шифрування.

**Алгоритмічно-програмне забезпечення шифрування даних у WiMAX-системах**

**Механізми захисту даних у WiMAX-системах.** Сьогодні прогресивно розвиваються підходи та механізми захисту даних у комунікаціях і системах безпроводного зв’язку четвертого покоління [10]. Конфіденційність, цілісність та доступність інформації у WiMAX-системах забезпечується використанням методів і засобів захисту апаратно-програмного рівня згідно зі стандартом IEEE 802.16e-2012, який передбачає [11, 12]:

- використання засобів протоколу EAP (*Extensible Authentication Protocol*) і алгоритму RSA (*Rivest, Shamir u Adleman*) для аутентифікації та авторизації абонентської станції;

- здійснення криптографічних перетворень трафіку для забезпечення конфіденційності та автентичності даних;
- використання протоколу керування ключами РКМ (*Privacy and Key Management protocol*) для безпечного розподілу ключової інформації.

Шифрування інформації в мережі WiMAX відбувається за допомогою ключа ТЕК (*Traffic Encryption Key*), який генерується протоколом РКМ. Дані розділяються на поля MAC PDU (*Media Access Control Protocol Data Unit*). Кожне поле складається із заголовка (*Generic MAC Header*), корисного навантаження та контрольної суми CRC (*Cyclic Redundancy Check*) і шифруванню підлягає лише корисне навантаження. У заголовок входить прапорець шифрування ЕС (*Encryption Control*), ключова послідовність ЕКС (*Encryption Key Sequence*) та ідентифікатор з'єднання СІД (*Connection Identifier*).

Сегмент ЕС показує, чи застосовується шифрування до поточного MAC PDU. Якщо значення прапорця дорівнює 1, то поле містить зашифроване корисне навантаження. В іншому випадку навантаження відсутнє або відкрите.

Сегмент ЕКС складається з двох бітів і містить номер поточного ТЕК. Базова станція періодично оновлює ключові послідовності, тому ТЕК має обмежений термін дії. Якщо корисне навантаження MAC PDU зашифроване за допомогою нового ключа, то у відповідному заголовку значення ЕКС зростає на 1 за модулем 4. Відповідно, легко вдається виявити збій синхронізації ключових послідовностей між базовою та абонентською станціями.

Шифрування даних відбувається в одному з чотирьох режимів, які відрізняються операціями над блоками даних, способом формування ініціалізувального вектора і можливістю аутентифікації:

- *Electronic CodeBook* (ЕСВ), який відповідає найпростішій схемі блокового шифрування;
- *Cipher-Block Chaining* (СВС) – передбачає побітову суму за модулем два результатів шифрування поточного блока з попереднім.
- *CounTeR* (СТР) – функціонує на основі шифрування унікальних ініціалізувальних векторів, які побітово додаються за модулем два до блока даних.
- *Counter with CBC-MAC* (ССМ) – поєднання режиму шифрування СТР та режиму аутентифікації СВС-МАС.

Сукупність алгоритмів шифрування та аутентифікації WiMAX утворює криптографічний комплекс, передбачений стандартом IEEE 802.16e-2012:

- на етапі аутентифікації:
- ASN (*Access Service Network*);
- AES у режимі ССМ із 128-бітним ключем;
- на етапі шифрування ключа ТЕК:
- 3-DES зі 128-бітним ключем;
- RSA зі 1024-бітним ключем;
- AES у режимі ЕСВ із 128-бітним ключем;
- на етапі шифрування даних:
- DES у режимі СВС з 56-бітним ключем;
- AES у режимах ЕСВ, ССМ, СВС, СТР із 128-бітним ключем;

Надійність функціонування кожного з етапів забезпечується використанням сучасного потокового алгоритму шифрування AES. Розглянемо засади програмної реалізації цього алгоритму в режимі ЕСВ у межах системної моделі безпеки технологій безпроводного зв'язку.

**Шифрування даних у WiMAX-системах: стандарт AES, мова програмування C#.** Розглянемо порівняльну характеристику сучасних блокових алгоритмів шифрування даних, які застосовуються в ІКТ, у контексті їх переваг та особливостей (див. таблицю) [13].

*Алгоритм шифрування AES.* AES (RIJNDAEL) – симетричний ітераційний алгоритм блокового шифрування. Стандартом AES передбачені розміри блока 128 біт і ключа 128/192/256 біт, а розмір ключа може відрізнитися від розміру блока. Особливості алгоритму AES такі:

- нова архітектура “Квадрат”, що забезпечує швидке розсіювання і перемішування інформації, при цьому за один раунд перетворюється весь вхідний блок;
- байт-орієнтована структура, зручна для реалізації на 8-розрядних мікроконтролерах;
- усі раундові перетворення допускають ефективну апаратну і програмну реалізацію на різних платформах.

## Порівняльна характеристика блокових алгоритмів шифрування

Назва алгоритму	Переваги	Особливості
<i>MARS</i>	<ul style="list-style-type: none"> <li>• високий рівень захищеності</li> <li>• висока ефективність на 32-розрядних платформах</li> <li>• потенційно підтримує розмір ключа більше ніж 256 бітів</li> </ul>	<ul style="list-style-type: none"> <li>• складність алгоритму</li> <li>• зниження ефективності на платформах без необхідних операцій</li> <li>• складність захисту від тимчасового аналізу й аналізу потужності</li> </ul>
<i>RC6</i>	<ul style="list-style-type: none"> <li>• висока ефективність на 32-розрядних платформах</li> <li>• проста структура алгоритму</li> <li>• наявність попередника – RC5</li> <li>• швидка процедура формування ключа</li> <li>• потенційно підтримує розмір ключа більше ніж 256 бітів</li> <li>• довжина ключа і кількість раундів можуть бути змінними</li> </ul>	<ul style="list-style-type: none"> <li>• порівняно низький рівень захищеності</li> <li>• зниження ефективності на платформах, що не мають необхідних операцій</li> <li>• складність захисту від тимчасового аналізу й аналізу потужності</li> <li>• відсутність можливості генерації раундових ключів у режимі реального часу</li> </ul>
<i>SEPRENT</i>	<ul style="list-style-type: none"> <li>• високий рівень захищеності</li> <li>• реалізація в smart-картах</li> </ul>	<ul style="list-style-type: none"> <li>• порівняно повільний</li> <li>• вразливий до аналізу потужності</li> </ul>
<i>TWOFISH</i>	<ul style="list-style-type: none"> <li>• високий рівень захищеності</li> <li>• реалізація у smart-картах</li> <li>• висока ефективність на будь-яких платформах</li> <li>• підтримує генерацію раундових ключів у режимі реального часу</li> <li>• підтримує паралельні операції на рівні інструкцій</li> <li>• допускає довільну довжину ключа до 256 бітів</li> </ul>	<ul style="list-style-type: none"> <li>• особливості алгоритму ускладнюють його аналіз</li> <li>• висока складність алгоритму</li> <li>• застосування операції додавання робить алгоритм вразливим до аналізу потужності й тимчасового аналізу</li> </ul>
<i>AES (RIJNDAEL)</i>	<ul style="list-style-type: none"> <li>• висока ефективність на будь-яких платформах</li> <li>• високий рівень захищеності</li> <li>• реалізація у smart-картах</li> <li>• швидка процедура формування ключа</li> <li>• підтримка паралелізму на рівні інструкцій</li> <li>• підтримка різних довжин ключа з кроком 32 біти</li> </ul>	<ul style="list-style-type: none"> <li>• вразливий до аналізу потужності</li> </ul>

Завдяки стійкості, продуктивності та ефективності реалізації AES широко застосовується на рівні шифрування даних у технологіях безпроводного зв'язку.

*Мова програмування C#: обґрунтування вибору.* Для програмної реалізації шифрування даних у безпроводних технологіях зв'язку зручно використати C#, яка має всі необхідні модулі та компоненти і такі переваги [14]: об'єктно-орієнтована мова програмування; належить до сім'ї мов з C-подібним синтаксисом; має статичну типізацію; підтримує анонімні функції з підтримкою замикань та винятки; має безпечну систему типів, які походять від C та C++; поєднує продуктивність *Visual Basic* та потужність C++; можливість використання делегатів, атрибутів, літераторів, анонімних функцій та узагальнених типів і методів; необмежена можливість успадкування та універсалізації; дає змогу створювати модульні програми з графічним інтерфейсом, використовуючи основні конструкції та стандартні типи даних, забезпечуючи сумісність платформ та швидкодію.

*Алгоритм шифрування даних у WiMAX-мережі.* Алгоритм шифрування даних наведено на рис. 2: *AddRoundKey ( )* – порозрядна операція XOR з поточним фрагментом розгорнутого ключа; *SubBytes ( )* – побайтова підстановка в S-блоках з фіксованою таблицею заміни розмірністю  $8 \times 256$ ; *ShiftRows ( )* – побайтовий зсув рядків масиву *State* на різну кількість байтів; *MixColumns ( )* – множення стовпців стану, що розглядаються як многочлени, на многочлен третього степеня  $g(x)$  за модулем  $x^4 + 1$ ; *AddRoundKey ( )* – порозрядна операція XOR з поточним фрагментом розгорнутого ключа.

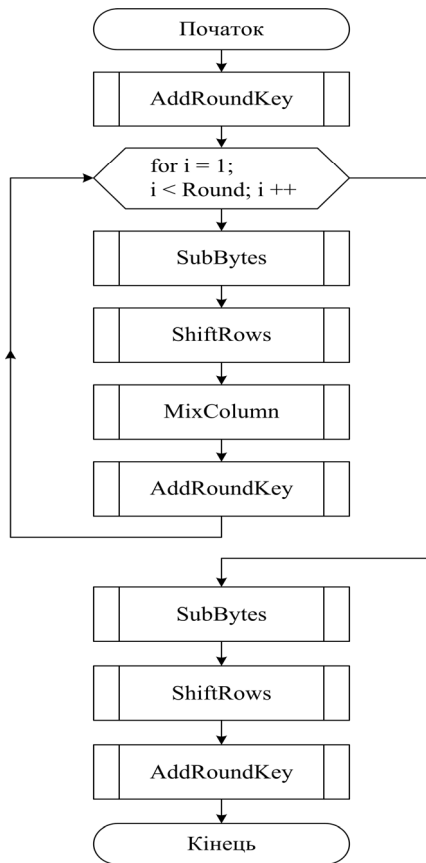


Рис. 2. Блок-схема алгоритму програмної реалізації шифрування AES

Блок-схема (рис. 2) показує послідовність класів і підпрограм алгоритму шифрування AES, який можна реалізувати засобами будь-якої об'єктно-орієнтованої мови програмування.

*Програмна реалізація.* Скріншот програмної реалізації шифрування даних у WiMAX-мережі показано на рис. 3.

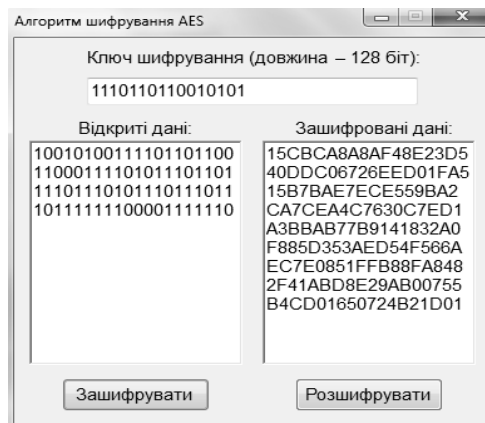


Рис. 3. Скріншот програмної реалізації шифрування даних у WiMAX-мережі

Алгоритмічно-програмне забезпечення процедури шифрування даних дасть змогу забезпечити достатній рівень інформаційної безпеки у WiMAX-мережі.

## Висновки

Запропоновано методологію захисту даних у технологіях безпроводного зв'язку на рівні системної моделі, яка дає змогу розв'язувати проблемні задачі функціональної та інформаційної безпеки даних у комунікаціях і цифрових системах на рівні метрологічно забезпеченої структури “системи – радіосигнали – радіоканали – тракти” згідно з концепцією “об’єкт – загроза – захист”. Проаналізовано механізми забезпечення захисту даних у WiMAX-системах. У сегменті програмного забезпечення системної моделі створено алгоритмічно-програмне забезпечення процедури шифрування даних у WiMAX-мережі на основі стандарту AES мовою програмування C#, що забезпечує конфіденційність, достовірність, цілісність даних у контексті функціональної та інформаційної безпеки технологій безпроводного зв'язку.

1. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 5 липня 1994 року № 80/94-ВР. Остання редакція від 19.04.2014. – [Електронний ресурс]. – Режим доступу: <http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>. 2. Постанова Кабінету Міністрів України “Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах” від 29.03.2006 № 373. Остання редакція від 13.10.2011. – [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/373-2006-%D0%BF>. 3. Чунарьова А. В. Аналіз існуючих шаблонів систем автентифікації в інформаційно-комунікаційних системах та мережах / А. В. Чунарьова, А. В. Чунарьов // *Безпека інформації: наук.-практ. журнал.* – 2012. – № 2 (18). – С. 65–70. 4. Оцінка якості відновлення мови в захищених безпроводових каналах зв'язку / [Коханович Г. Ф., Голубничий О. Г., Одаренко Р. С., Беженар Ю. В.] // *Безпека інформації: наук.-практ. журнал.* – 2012. – № 1. – С. 37–41. 5. Параметры прогнозирования и идентификации атак в информационно-коммуникационных системах / [Азарсков В. Н., Гизун А. И., Грехов А. М., Скворцов С. А.] // *Научно-практический журнал “Защит информации”.* – 2014. – Т. 16. – № 1. – С. 89–95. 6. Корченко А. О. Система виявлення та ідентифікації порушника в інформаційно-комунікаційних мережах / А. О. Корченко, В. В. Волянська, Гізун А. І. // *Научно-практический журнал “Безпека информации”.* – 2013. – Т. 19. – № 3. – С. 158–162. 7. Шевченко А. С. Метод оцінювання ризиків з урахуванням впливу механізмів захисту інформації на параметри безпроводових інформаційно-телекомунікаційних систем під час інформаційних операцій / А. С. Шевченко, О. В. Кокотов // *Научно-практический журнал “Безпека информации”.* – 2014. – Т. 20. – № 1. – С. 7–11. 8. Славінський С. Деякі питання метрологічного забезпечення у цифрових телекомунікаціях й системах зв'язку / С. Славінський // *Стандартизація, сертифікація, якість.* – 2009. – № 3. – С. 28–34. 9. Системна безпека технологій безпроводного зв'язку: моделі загроз та захисту мовної інформації / [Дудікевич В. Б., Микитин Г. В., Ребець А. І., Банах Р. І.] // *Матеріали III міжнародної науково-технічної конференції “Защит информации і безпека інформаційних систем”.* – Львів, 5–6 червня, 2014. – С. 50–51. 10. Лавровская Т. В. Анализ методов повышения защищенности в LTE-системах / Т. В. Лавровская // *Системы обработки информации.* – 2014. – Вып. 5 (121). – С. 139–141. 11. IEEE Standard for Air Interface for Broadband Wireless Access Systems: IEEE 802.16-2012. – [Approved 8 June 2012]. – New York, NY: The Institute of Electrical and Electronics Engineers, Inc., 2012. – 2544 p. 12. Рашич А. В. Сети беспроводного доступа WiMAX: учеб. пособие / Рашич А. В. – СПб.: Изд-во Политехн. ун-та, 2011. – 179 с. 13. Зенин О. С. Стандарт криптографической защиты – AES. Конечные поля / О. С. Зенин, М. А. Иванов; под ред. М. А. Иванова. – М.: КУДИН-ОБРАЗ, 2002. – 176 с. 14. Павловская Т. А. С#. Программирование на языке высокого уровня: учебник для вузов / Т. А. Павловская. – СПб.: Питер, 2009. – 432 с.