

МОДЕЛЬ ТА СТРУКТУРНО-ФУНКЦІОНАЛЬНИЙ СКЛАД ТЕРМІНАЛУ РАДІОДОСТУПУ ПРИ ДОСЛІДЖЕННЯХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В CROSS-П РС ДСВМ В УМОВАХ РАДІОЕЛЕКТРОННОЇ ПРОТИДІЇ

Казакова Н.Ф.¹, к.т.н., доцент, Грабовський О.В.², к.т.н., доцент.

1 – Одеський національний економічний університет,

**2 - Одеська державна академія технічного регулювання та якості,
м. Одеса**

Враховуючи різноманітність послуг (екзофакторів), які у майбутньому будуть надаватися у державному секторі відкритої мережі (ДСВМ) засобами cross-платформених радіоструктур (Cross-П РС), у якості кінцевого пристрою (ендофактора), який отримує послугу, може бути використано захищений складений пристрій (ЗСП), суть функціонування якого приводиться нижче. У якості його прототипу обрано варіант побудови для системи мобільного зв'язку стандарту GSM, який описано в [1] та приведено у доповіді.

В основу функціонування ЗСП покладено діючий державний стандарт ГОСТ 28147-89, який вимагає забезпечення необхідної безпеки при обміні інформацією між абонентами за принципом «точка-точка» [2-4]. При цьому враховано, що одним з доступних і досить добре описаних у науковій та технічній літературі є алгоритм шифрування повідомлень у системі мобільного стільникового зв'язку (СМСЗ) стандарту CDMA, який відповідає зазначеному стандарту. У процесі досліджень [5, 6] було встановлено, що в силу ряду причин, використовуваний алгоритм є неприйнятним для абонентів комп'ютерних мереж, які вимагають використання інших алгоритмів шифрування, зокрема таких, що відповідають не широкосмуговим радіосистемам, а кабельним з обмеженою смугою пропускання. Відповідно, не порушуючи завдань, поставлених до дослідження стосовно впливу систем радіоелектронного придушення на засоби ДСВМ [7, 8], результати експериментальних досліджень і програмного моделювання процесів переносу спектра в область дуже високих частот (ДВЧ), а також датчиків псевдовипадкових та хаотичних сигналів, було вирішено віднести тільки до радіозасобів та до проблем порушення процесів синхронізації [9] на відповідних його ділянках.

Як випливає з [1], можливість передачі даних закладена в будь-якому терміналі стандартів CDMA та GSM. Враховуючи це, було ухвалено рішення про те, що доцільним для експериментальних досліджень може буде такий спосіб засекречування, коли деякий програмно-апаратний пристрій (ПАП), підключається через порт EIA232 до базового телефону стандарту CDMA, утворюючи в сукупності ЗСП. У такому пристрої (П₁, рис. 1) інтегруються вже готовий високоякісний кодек, система шифрування, вбудовані алгоритми завадостійкості, порт RS-232C для підключення периферійних пристроїв передачі повідомлень та сигналів контролю й управління, а також пристрій узгодження з інтерфейсом базового радіотелефону стандарту CDMA, що працює з використанням відповідного протоколу. Цей спосіб організації ЗСП вважався базовим варіантом. Аналогічну структуру досліджено в [1], де в якості ЗСП використано термінал стандарту GSM.

При експериментальних дослідженнях такий структурно-функціональний склад терміналу радіодоступу до екзофакторів ДСВМ забезпечив незалежну від системи мобільного зв'язку безпеку засекречених з'єднань, а відсутність радіоінтерфейса в P_1 та P_2 дозволило спростити їх електричну схему, що, у перспективі при масовому випуску терміналів, може привести до підвищення технологічності виробництва, знизити вартість та масогабаритні характеристики [10].

У якості базового радіоустаткування використано ряд різноманітних радіотерміналів стандарту CDMA, що працюють у стандартному діапазоні. ЗСП з пристроєм введення ключа, що перебував в персональній sim-картці (а саме – в P_1), вважався ендофактором. Аналогічно P_2 був визначений, як екзофактор. Було враховано зауваження з [1] про те, що при використанні стандартного радіотелефону, недоліком є його функціональна надмірність. Так, відповідно до рис. 1, при підключенні використовується тільки режим передачі даних, а такі складові частини, як мікротелефон або інше джерело сигналу («Вхід 1», «Вихід 1», «Вхід 2», «Вихід 2» на рис. 1) та кодек часто не використовуються, але вносять свої складові в загальну шумову компоненту.

При використанні спеціальних абонентських пристроїв передавання даних, вище зазначений недолік усувається шляхом установки стандартних PCMCIA карт в портативний комп'ютер (якщо він виступає в якості ендофактора). У цьому випадку, тобто при передаванні/прийманні, наприклад, сигналів управління для C31, P_1 та P_2 повинні мати інтерфейси PCMCIA та відповідне програмне забезпечення. Це вважали «варіантом 1» з'єднання «точка-точка», який підлягав дослідженням. Його достоїнство – максимально прості ЗСП. Ряд фірм випускає радіомодеми GSM, підключивши до яких P_N за допомогою кабеля через порт RS232, можна отримати ЗСП у вигляді закінченого пристрою. Враховуючи це, немає принципових труднощів для виготовлення аналогічних радіомодемів для стандарту CDMA. Таке підключення вважали «варіантом 2». Подібні радіомодеми (для стандарту GSM) виконані у вигляді модулів, що мають 2 рознімання для послідовного порту та зовнішньої радіоантени. Для потреб експерименту робота модему стандарту CDMA імітувалася стандартною програмною підсистемою з набору підпрограм відкритого середовища OpenCV. Взаємодія терміналів P_1 та P_2 здійснювалася через послідовний порт з різними швидкостями в межах встановленого спектра частот, а отримані результати порівнювалися з результатами, отриманими в [1] для швидкості 9,6 кБіт/с.

Програмне управління моделлю модему стандарту CDMA здійснювалося за допомогою команд, що включають стандартний набір AT-команд. Ними здійснювалася установка pin-коду, проводився вибір каналу в мережі, виділялася інформація про параметри радіополя та про ряд інших функцій, характерних для будь-якого радіотерміналу, коректувалася робота системи синхронізації, вибір системи шифрування, задавалися розміри таблиць кодування Уолша та ін. Отримані результати щодо комплексного показника оцінки якості в залежності від ймовірності помилки демонструються у доповіді у вигляді графіків.

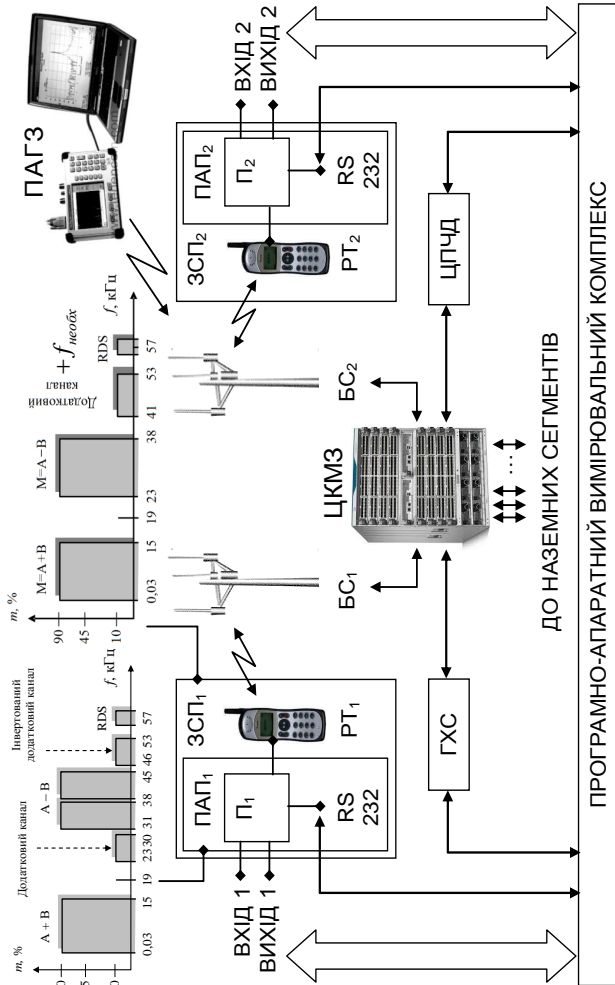


Рис. 1. Спрощена експериментальна схема організації зв'язку за принципом «точка-точка» через СМСЗ стандарту CDMA, де: ЗСП₁, ЗСП₂ – захищені складені пристрої; БС₁, БС₂ – базові станції; П₁, П₂ – інтегровані пристрої шифрування; РТ₁, РТ₂ – радіотелефони стандарту CDMA; ЦКМЗ – дослідний центр комутації мобільного зв'язку; ПАГЗ – програмно-апаратний генератор завад; ПАП₁, ПАП₂ – програмно-апаратні пристрої; ЦПЧД – цифровий прецизійний числовий дискриміноватор; ГХС – програмно-апаратний генератор хаотичних сигналів

Література

1. Назаров А. Н. Алгоритмы некриптографической защиты информации при доставке сообщений в системе подвижной сотовой связи в условиях радиоэлектронного противодействия [Електронний ресурс] / А. Н. Назаров, А. Б. Сикорский, Е. И. Деркач // Портал : без назви. – Режим доступу \www/URL:http://www.ssl.stu.neva.ru/ssl/publications/magazine/2002/4/5/nazarov.pdf. – Заголовок з контейнера, доступ по пароллю, 21.09.2014.
2. Казакова Н. Ф. Оцінка живучості систем моніторингу інформаційного простору [Текст] / Н. Ф. Казакова // Восточно-европейский журнал передовых технологий. – 2012. – № 4/2(58). – С. 12-15.
3. Казакова Н. Ф. Априорна суперечність раціональної концепції інтелектуальної мережі [Текст] / Н. Ф. Казакова // Управління проектами: стан та перспективи : міжнар. наук.-техн. конф., 2008 : матер. конф. – Миколаїв, НУК ім. адмірала Макарова. – С. 65-67.
4. Казакова Н. Ф. Анализ эффективности информационных систем путем синтеза критериев оптимизации алгоритмов их функционирования [Текст] / Н. Ф. Казакова, И. О. Годулян, А. А. Чуприна // Сучасні телекомунікаційні та інформаційні технології : II наук.-практ. семін. молодих науковців та студентства, 12-14 грудня 2007 р. : матер. семін. – Київ, УНДІЗ.
5. Казакова Н. Ф. Методика организации идеального профилактического обслуживания [Текст] / Н. Ф. Казакова // Системы синхронизации, формирования и обработки сигналов для связи и вещания : науч.-техн. семин., 1-4 июня 2007 г. : матер. семин. : под ред. В. В. Шахгильдяна. – Москва–Одесса, IEEE-РНТОРЭС им. А. С. Попова. – С. 167-172.
6. Казакова Н. Ф. Управління послугами телекомунікацій [Текст] / Н. Ф. Казакова // II звітна наук.-практ. конф. проф.-викл. складу та студентства Міжнар. гуманіт. ун-ту, 12 квітня 2007 р. : матер. конф. – Одеса, Міжнар. гуманіт. ун-т. – С. 18-21.
7. Казакова Н. Ф. Задачі захисту інформаційних ресурсів від впливу зовнішніх загроз [Текст] / Н. Ф. Казакова // Сучасні інформаційні технології в повсякденній діяльності та підготовці фахівців : II молод. наук. конф., 31 березня 2006 р. : матер. конф. – Одеса, ОНЮА. – С. 45-47.
8. Казакова Н. Ф. Аналіз внутрішніх та зовнішніх загроз корпоративних мереж [Текст] / Н. Ф. Казакова // Технічні засоби захисту інформації : міжвідомч. міжрегіон. семінару Наукової Ради НАН України, 15 лютого 2006 р. : матер. семін. – Київ-Одеса, НАН України. – С. 11.
9. Казакова Н. Ф. Принципи створення систем мережного управління [Текст] / Н. Ф. Казакова // Актуальні проблеми та досвід використання сучасних інформаційно-комунікаційних технологій : наук.-практ. конф. проф.-викл. складу, 10-12 травня 2005 р. : матер. конф. – Одеса, ОНЮА. – С. 133-138.
10. Казакова Н. Ф. Особенности расчета показателей надежности компьютерных устройств управления резервным оборудованием [Текст] / Н. Ф. Казакова // Системний аналіз та інформаційні технології : VI міжнар. наук.-практ. конф. студентів, аспірантів та молодих вчених ІПСА-2004, 1-3 липня 2004 р. : матер. конф. – Київ, НТУУ «КПІ». – С. 209-210.