

УДК 004.056.5

**В. Ф. Бардаченко, д. т. н., проф.; В. В. Поліновський, магістр**  
**ЗАСТОСУВАННЯ ТАЙМЕРНИХ МЕТОДІВ ДЛЯ КОДУВАННЯ**  
**АУДІОДАНИХ У КОМП'ЮТЕРНІЙ ТЕЛЕФОНІЇ**

Одним із провідних напрямків розвитку телекомунікаційних технологій є інформаційна безпека й формування служб і завдань комп'ютерної телефонії з підвищеною безпекою. Значно зменшити вартість інформаційного захисту й підвищити його ефективність дозволяє методологія, в основі якої лежить ідентифікаційний ключ Бардаченка (ВІК). Розглянуто розроблені алгоритми кодування інформації, засновані на ВІК з використанням таймерних методів. Розроблені алгоритми показали на практиці ефективність використання таймерних методів кодування інформації, що дозволить абонентів комп'ютерної телефонії захистити дані від несанкціонованого доступу й розшифрування аудіоданих.

### Вступ

На думку експертів в області інформаційної безпеки [1] хакери шукають найкоротший шлях для злому на вигляд навіть незламних мереж. Найчастіше вони підслуховують телефонні розмови і читають пошту їхніх користувачів, щоб перехоплювати паролі й інші важливі дані для доступу до корпоративних баз даних або банківських рахунків.

Приклад того, як можна отримати доступ до секретної інформації, продемонстрував арештований на початку цього місяця житель Каліфорнії, що зламав базу даних стільникової мережі оператора T-Mobile, а після цього читав пошту і файли, що пересилаються американськими спецслужбами.

Хакери все частіше починають перехоплювати секретну інформацію, що передається через телекомунікаційні сервери, особливо ті, що забезпечують безпроводний доступ в мережу Інтернет. Телеком-оператори є на сьогоднішній день одними з основних об'єктів хакерських атак — адже саме вони забезпечують усі види зв'язку, якими користуються люди, незалежно від роду діяльності і службового становища.

Щоб отримати доступ до телефонної мережі, хакери представляються технічними фахівцями телефонної компанії й одержують паролі для доступу. Таким чином, вони можуть прослуховувати телефони або перехоплювати пошту абонентів — текстові документи або навіть фотографії з камерофонів, повідомляє Reuters [2].

Тому, одним з провідних напрямків розвитку телекомунікаційних технологій є *інформаційна безпека* і формування служб і задач комп'ютерної телефонії з підвищеною безпекою.

Інформаційна безпека містить у собі вирішення таких задач:

- забезпечення конфіденційності інформації;
- забезпечення вірогідності інформації;
- забезпечення оперативності доступу до інформації;
- забезпечення невідстежуваності дій клієнта.

Традиційно для розв'язання задач телекомунікаційної безпеки застосовуються скремблери, маскиратори або криптофони [3]. При цьому найчастіше для роботи таких пристроїв необхідна аутентифікація користувача, що найчастіше відбувається за відбитком пальця, криптопаролем, електронним підписом тощо.

Методика захисту за допомогою пароля і/або електронного підпису має свої переваги і недоліки. До переваг відноситься зручність і відносно, у порівнянні з методами аутентифікації, невелика вартість таких систем, однак, цей захист має низку недоліків, пов'язаних з утаємненням паролів від користувачів, що не мають права доступу. Ідеально вирішує проблему прав доступу захист за допомогою аутентифікації. Але такі системи мають досить високу вартість, що примусило значну кількість потенційних споживачів, які потребують надійного захисту своєї інформації за допомогою аутентифікації, відмовитися від їх використання.

Значно зменшити вартість інформаційного захисту і підвищити її ефективність дозволяє методологія, в основі якої лежить ідентифікаційний ключ Бардаченко (ВІК), показаний на рис. 1.

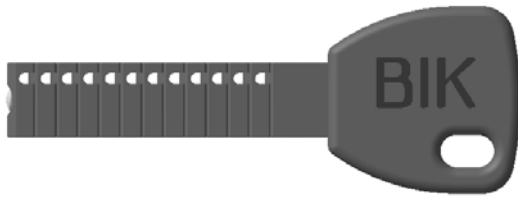


Рис. 1. Ідентифікаційний ключ Бардаченко (ВІК)

### Основна частина

Розглянемо докладніше застосування таймерних методів для кодування аудіоданих. За базовий метод, для якого ми будемо використовувати таймерні методи, візьмемо метод змішування аудіоданих. Використовуючи цей метод, аудіопотік розбивається на ділянки по 0,3 секунди, кожна з яких поділяється на чотири частини, а ці частини змішуються певним чином. При цьому методів змішування всього 12, але прийнятними є тільки 8.

Розглянемо докладніше алгоритм з елементами таймерних методів, названий умовно «класичним», тому що він найбільш схожий на класичний алгоритм змішування. Для роботи з цим алгоритмом необхідно визначити довжини вибірок і спосіб їх змішування, ці параметри задаються за допомогою ВІК.

Для роботи з «класичним» алгоритмом потрібно два введення ключа Бардаченко, разом виходить 24 розряди. З цих 24 розрядів 21 розряд задають довжини вибірок, по 7 розрядів на кожну з трьох вибірок, четверта ж вибірка визначається як залишок; а 3 розряди визначають спосіб змішування вибірок.

Розглянемо докладніше, як визначаються довжини вибірок. Весь звуковий потік поділяється на ділянки  $B$ , довжиною по 0,3 сек. Кожна з  $B$ -ділянок поділяється на 10 частин (рис. 2).

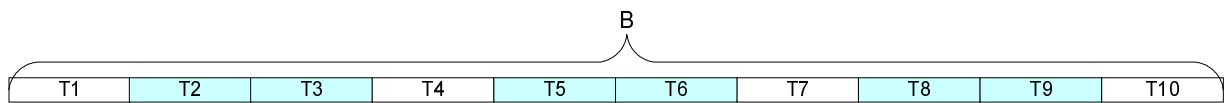


Рис. 2. Ділянка  $B = 0,3$  с

Ділянки  $T_1$ ,  $T_4$ ,  $T_7$  і  $T_{10}$  є основами або базовими відрізками для формування чотирьох вибірок. Ділянки  $T_2 + T_3$ ,  $T_5 + T_6$  і  $T_8 + T_9$  поділяються на 128 частин, тобто максимальне число, яке можна задати 7-ма розрядами у двійковому численні (рис. 3).

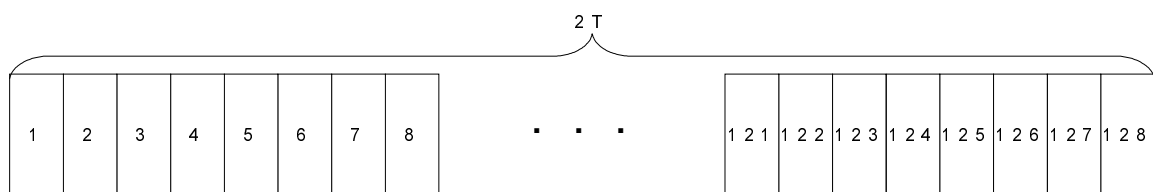


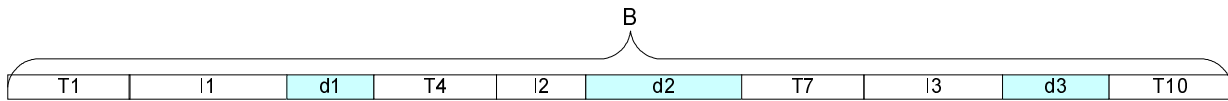
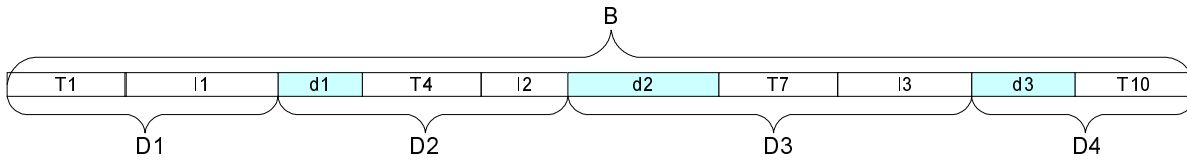
Рис. 3. Здвоєні ділянки

З цих 128 частин формуються доповнення  $I_n$  (додаткові відрізки) до базових вибірок, для цього вибирається стільки частин, скільки задано 7-ма розрядами ключа Бардаченка. У даному випадку для  $I_1$  використовуються розряди з 1 по 7, для  $I_2$  — з 8 по 15, а для  $I_3$  — з 16 по 21. При цьому стає очевидним, що з метою безпеки можна використовувати абсолютно інші розряди для формування довжин вибірок.

Отже, після розподілу на частини кожної з пар  $T_2 + T_3$ ,  $T_5 + T_6$  і  $T_8 + T_9$  і вибірок з них  $I_1$ ,  $I_2$  і  $I_3$  відповідно ділянку  $B$  можна представити у вигляді, показаному на рис. 4.

При цьому,  $d_1$ ,  $d_2$  і  $d_3$  — це залишки від  $2T$  після визначення  $I_1$ ,  $I_2$  і  $I_3$  відповідно. Після цього залишається сформувати чотири вибірки  $D_1$ ,  $D_2$ ,  $D_3$  і  $D_4$ , що будуть змішуватися (рис. 5).

Очевидно, що для визначених ключів розміри  $d$  або  $I$  можуть бути нульові або ж розмір залишку може бути більшим, ніж сума базового і додаткового відрізків.

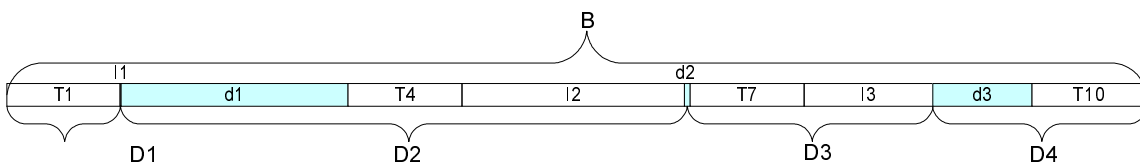
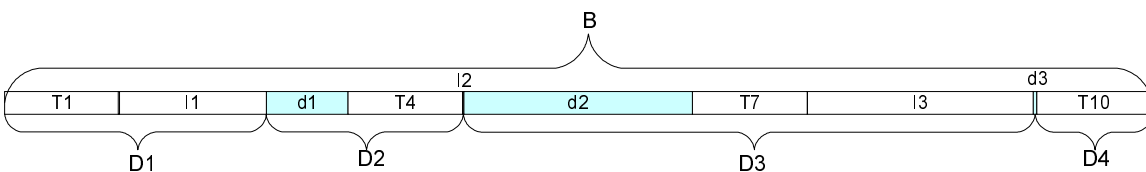
Рис. 4. Ділянка  $B$  після розподілу на частиниРис. 5. Ділянка  $B$  з виділеними вибірками  $D_1, D_2, D_3$ 

Після визначення довжин вибірок відбувається їхнє змішування відповідно до методу, що був обраний 3-ма розрядами на ключі Бардаченка. У нашому прикладі це 22, 23 і 24 розряди, хоча варто згадати про те, що з метою безпеки це можуть бути зовсім інші розряди.

З використанням даного алгоритму була написана програма з кодування і розкодування звукових повідомлень. Після тривалого ряду експериментів з кодуванням і розкодуванням звукових повідомлень з різними наборами ключа ВІК у даного алгоритму виявився ряд недоліків.

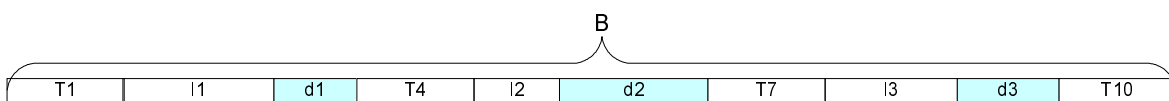
У дуже великому інтервалі  $D_i$  підвищується можливість розпізнавання мови або, принаймні, вдається вихопити окремі звукосполучення й вловити зміст повідомлення.

Такі ситуації виникають, коли  $I_{n-1}$  прагне до нуля, у той час як  $I_n$  — до максимального значення. Причому очевидно, що найбільше цей негативний ефект буде виявлятися на відрізках  $D_2$  і  $D_3$ , рис. 6 і 7 відповідно

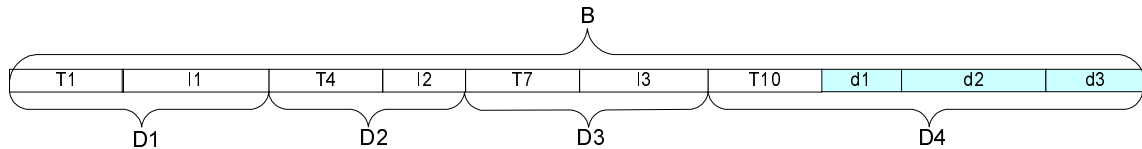
Рис. 6. Відрізок  $D_2$  прагне до максимумуРис. 7. Відрізок  $D_3$  прагне до максимуму

З метою виправлення недоліків «класичного» алгоритму був запропонований і розроблений «альтернативний» алгоритм. Для роботи з цим алгоритмом також потрібно два введення ключа Бардаченка. Цей алгоритм нагадує «класичний» алгоритм, відмінність тільки у формуванні кінцевих чотирьох вибірок. Тому саме цей момент і розглянемо докладніше.

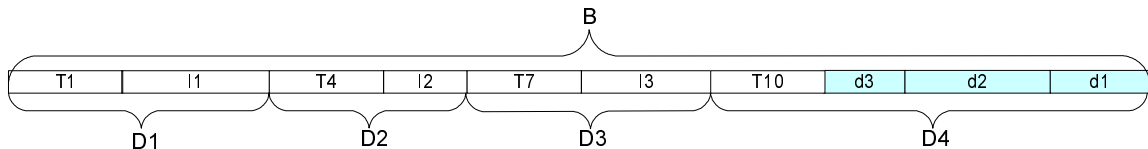
Отже, після розподілу на частини кожної з пар  $T_2 + T_3$ ,  $T_5 + T_6$  і  $T_8 + T_9$  і вибірок з них  $I_1$ ,  $I_2$  і  $I_3$  відповідно ділянку  $B$  можна представити у вигляді, показаному на рис. 8.

Рис. 8. Ділянка  $B$  після розподілу

При реалізації альтернативного алгоритму всі залишки  $d$  послідовно переміщуються в кінець ділянки  $B$  і формують вибірку  $D_4$ . При цьому виникає ситуація, показана на рис. 9.

Рис. 9. Вибірка  $D_4$  із залишками  $d$ 

Можна також не подавати залишки послідовно в кінець  $Y$ , а перемішати їх між собою (рис. 10).

Рис. 10. Вибірка  $D_4$  з перемішаними залишками  $d$ 

Метод змішування такий же, як і в «класичному» алгоритмі, тобто, відповідно до методу, що був обраний 3-ма розрядами на ключі Бардаченка. У нашому прикладі це 22, 23 і 24 розряди, хоча варто згадати про те, що з метою безпеки це можуть бути зовсім інші розряди.

### Висновок

Наведені алгоритми показали на практиці ефективність використання таймерних методів кодування інформації, що дозволить абонентові комп'ютерної телефонії захистити дані від несанкціонованого доступу або перехоплення і розшифровки аудіоданих.

Надалі планується провести глибше дослідження розглянутих алгоритмів на швидкість і ефективність кодування й розкодування аудіоданих. А також створення програмно-апаратного комплексу для формування служб і задач комп'ютерної телефонії з підвищеною безпекою.

### СПИСОК ЛІТЕРАТУРИ

1. Люди говорять, хакери слухають. Mode of access: Word Wide Web URL: <http://www.cnews.ru/newtop/index.shtml?2005/01/26/173490>
2. Mode of access: Word Wide Web URL: [http://www.cnews.ru/cgi-bin/redirect.cgi?%20http://www.rbc.ru/info/info\\_reuters.shtml](http://www.cnews.ru/cgi-bin/redirect.cgi?%20http://www.rbc.ru/info/info_reuters.shtml)
3. Давлетханов М. Прослуховування мобільника: захисти себе сам. Mode of access: Word Wide Web URL: <http://dago.nad.ru/article.php?storyid=817> [=DaGo=-] — комп'ютерна безпека.

Матеріали статті рекомендовані до опублікування оргкомітетом конференції «Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування» (2—5. 07.05)

Надійшла до редакції 11.07.05  
Рекомендована до друку 21.07.05

**Бардаченко Віталій Феодосійович** — директор Центру, **Поліновський В'ячеслав Васильович** — старший науковий співробітник.

Центр таймерних обчислювальних систем Інституту кібернетики ім. В.М. Глушкова НАН України