УДК 004.4'277.2.056.55

А. О. Азарова
І. Л. Медяна

РОЗРОБЛЕННЯ ПІДХОДУ ДО ЗАХИСТУ ЗВУКОВОЇ ІНФОРМАЦІЇ З МІКРОФОНУ ІЗ ЗАСТОСУВАННЯМ ЦИФРОВОГО КРИПТОГРАФІЧНОГО МЕТОДУ ШИФРУВАННЯ

Вінницький національний технічний університет

Анотація

Одним із важливих напрямків застосування методів кібербезпеки є захист звукової інформації. Аналіз існуючих методів та засобів вирішення такої проблеми дозволив виявити відповідні перспективні напрямки, зокрема, доведено єфективність використання цифрових криптографічних методів шифрування для захисту звукової інформації, що передається цифровими лініями зв'язку. У дослідженні застосовано модифікований метод однократного гамування, що уможливило розроблення відповідного програмного забезпечення для потокового шифрування звукової інформації з мікрофону. Цей підхід дозволяє користувачеві отримати такі переваги, як: збільшення швидкості шифрування та довжини ключа, високу крипостійкість програми; зручний інтерфейс запропонованого ПЗ.

Ключові слова: безпека, цифрові криптографічні методи, потокове шифрування, захист інформації.

Abstract

One of the important areas of application of cybersecurity methods is the protection of audio information. The analysis of the existing methods and means of solving such a problem allowed to reveal the corresponding perspective directions, in particular, the efficiency of the use of digital cryptographic encryption methods for the protection of sound information by digital communication was proved. The study used a modified method of one-time jamming, which allowed the development of appropriate software for streaming encryption of audio information from the microphone. This approach allows the user to obtain such advantages as: increase in encryption speed and key length, high cryptography of the program; user-friendly interface of the proposed software.

Keywords: security, digital cryptographic methods, streaming encryption, information security.

Вступ

В умовах бурхливого розвитку техніки та економіки поняття "безпека" здобуває розширеного змісту і містить у собі такі складові, як фізична, юридична й інформаційна безпека. Особливе місце посідає інформаційна безпека, що зумовлено зростаючою роллю інформації в житті суспільства. Отже, головними стають нематеріальні ресурси, зокрема, інформація. Інформаційні ресурси є об'єктами власності громадян, організацій, громадських об'єднань, держави.

Багатоваріантність побудови інформаційних систем дозволяє продукувати різні рішення у сфері розроблення систем захисту інформації. Широкомасштабне використання обчислювальної техніки і телекомунікаційних систем у межах територіально розподіленої мережі, перехід на цій основі на безпаперові технології, збільшення обсягів інформації, кількості користувачів призводить до того, що необхідно значно підвищувати рівень захисту інформації. При цьому важливим напрямком роботи фахівців із кібербезпеки є захист саме звукової інформації.

Основний зміст

На сучасному етапі розвитку криптографічних методів захисту для вирішення проблеми захисту звукової інформації можливо застосовувати два основних методи шифрування – аналоговий та цифровий. Разом із тим, аналогові пристрої криптографічного захисту – скремблери – мають значні недоліки. Цифрові пристрої криптографічного захисту, які реалізують метод цифрового шифрування, – вокодери – є істотно більш стійкими до дешифрування. У них сигнал попередньо перетворюється на цифровий вигляд. До каналу зв'язку передається набір стандартних знаків (як правило, нулів й одиниць). Для кодування подібних сигналів застосовуються значно більш складні й витончені системи ключів.

Криптографічні методи асиметричного шифрування мають значні недоліки, а саме:

- значно нижча швидкість ніж у симетричних;
- вимагають більше обчислень.

Вибір авторами дослідження серед методів шифрування саме симетричного – потокового шифрування – зумовлений тим, що він є швидкісним, просто реалізується, потребує меншої довжини ключа для порівняння стійкості.

Таким чином, аналіз відомих алгоритмів і схем криптографічного захисту інформації дозволив обґрунтувати вибір саме методу однократного гамування, який було застосовано для створення безпеки звукової інформації з мікрофону. Було розроблено відповідний програмний засіб. За мовну платформу було обрано Visual C++. Розроблений ПЗ дозволяє шифрувати звук як безпосередньо з мікрофона, так і зі звукових файлів WAV-формату і передбачає використання секретного масиву випадкових чисел великого розміру (до 1 Гбайта), який користувач може постійно носити із собою у вигляді флеш-пам‘яті та короткого паролю (напр., 8 символів), який треба пам‘ятати і не розголошувати.

Тестування програми показало, що швидкодія процесу шифрування склала близько 4 МБ/сек., що є цілком придатним для використання в реальному масштабі часу.

Перевагами застосування даної розробки користувачем є:

– збільшення швидкості шифрування. Оскільки в програмі використовується не генерація випадкових чисел, а вибір їх з готового масиву, то програма уможливлює більшу швидкість шифрування інформації;

– збільшення довжини ключа. Внаслідок використання ключа більшої довжини (128 біт замість 96) збільшується крипостійкість програми;

– простота використання програми. Завдяки наявності зручного інтуїтивного графічного інтерфейсу, засобами якого користувач може вводити власні початкові дані або вибирати їх з бази даних, підключеної до системи, необхідно лише слідувати простим рекомендаціям, що пропонуються. При цьому також зменшується кількість помилок оператора-користувача, що можуть бути здійснені на початкових етапах роботи із системою.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації: навчальний посібник. Харків : ХНЕУ, 2013. 476 с.

2. Основи криптографічного захисту інформації: підручник / Гулак Г. М., Мухачов В. А., Хорошко В. О., Яремчук Ю. Є. Вінниця: ВНТУ, 2011. 199 с

3. Франчук В. М. Захист інформаційних ресурсів: криптографічні та стеганографічні методи захисту даних. Посібник для викладачів, вчителів та студентів інформатичних спеціальностей. К. : НПУ імені М.П. Драгоманова, 2012. 120 с.

4. Глинчук Л. Я. Криптологія: навч.-метод. посіб. Луцьк : Вежа-Друк, 2014. 164 с.

5. Бурячок В. Л., Киричок Р. В., Складанний П. М. Основи інформаційної та кібернетичної безпеки. К., 2018. 320 с.

6. Яремчук Ю. Є. Методи та засоби шифрування інформації на основі рекурентних послідовностей : Автореф. дис... канд. техн. наук : 05.13.21. Ін-т пробл. моделювання в енергетиці НАН України. К., 2000. 20 с. укр.

7. Яремчук Ю. Є. Оцінювання криптостійкості методів шифрування інформації на основі рекурентних послідовностей. *Вост.-Европ. журн. передовых технологий*. 2013. № 2/10. С. 35 – 38. Бібліогр. : 10 назв. укр.

8. Azarova A., Azarova L., Rosol N., Bystritskiy O. Models and methods of electronic digital signature. Theoretical and scientific foundations of engineering : collective monograph / International Science Group. Boston : Primedia eLaunch, 2020. 180 p. P. 24 – 33. Available at :DOI:10.46299/isg.2020. MONO.TECH.II.

9. Азарова А. О., Азарова Л. Є., Білий Р. О., Міронова Ю. В. Комп’ютерна програма «Захищений засобами двофакторної авторизації месенджер для організації комінікаційних процесів на підприємстві». Свідоцтво про реєстрацію авторського права на твір №97856. Дата реєстрації 05.06.2020 р. Заявка № 99244 від 02.06.2020 р.

10. Азарова А. О., Азарова Л. Є., Білий Р. О., Міронова Ю. В. Комп’ютерна програма «Процедура реєстрації у захищеному месенджері для організації комунікаційних процесів на підприємстві». Свідоцтво про реєстрацію авторського права на твір № 97857. Дата реєстрації 05.06.2020 р. Заявка №99245 від 02.06.2020 р.

11. Азарова А. О., Азарова Л. Є., Білий Р. О., Міронова Ю. В. Комп’ютерна програма «Отримання та надсилання повідомлень користувачами у створеному месенджері для реалізації комунікаційного процесу на підприємстві». Свідоцтво про реєстрацію авторського права на твір № 97858. Дата реєстрації 05.06.2020 р. Заявка № 99246 від 02.06.2020 р.

12. Азарова А. О., Гудзь В. О., Блонський В. О. Управління та адміністрування захистом інформації шляхом локалізації закладних пристроїв на основі індитикатора електромагнітних випромінювань. Тези XLVIII науково-технічної конференції ВНТУ. 2019. URL : https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/view/7335/6122

13. Азарова А. О., Чайковська Я. В. Вдосконалення методу вбудовування цифрових водяних знаків на основі квантування для підвищення рівня захисту PDF файлів. Тези XLVIII науково-технічної конференції ВНТУ. 2019. URL : https://conferences. vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/view/7828

14. Азарова А. О., Азарова Л. Є., Каплун І. С., Щербатюк А. В. Свідоцтво про реєстрацію авторського права на твір №79707. Розробка контролеру кодового доступу до сейфа на мікроконтролері Arduino. Заявка від 05.06.2018 р. №80960. Дата реєстрації 14.06.2018 р.

Анжеліка Олексіївна Азарова – канд. техн. наук, професор, заст. декана Факультету менеджменту та інформаційної безпеки з наукової роботи та міжнародного співробітництва Вінницького національного технічного університету.

Azarova A. Anzhelika – Ph.D., Professor, Deputy dean of the Faculty of management and information security by scientific work and international cooperation Vinnytsia National Technical University, Vinnytsia.

Ірина Леонідівна Медяна – студентка Факультету менеджменту та інформаційних технологій Вінницького національного технічного університету, м. Вінниця, e-mail:fm.ub16.mediana@gmail.com

Iryna L. Mediana – student at the Faculty of Management and Information Technology, Vinnytsia national technical university, Vinnitsa.