УДК 004.4'277.2.056.55

І. Л. Медяна[1]

ОГЛЯД ІСНУЮЧОЇ ПРОБЛЕМАТИКИ ПОТОКОВОГО ШИФРУВАННЯ ЗВУКОВОЇ ІНФОРМАЦІЇ

Вінницький національний технічний університет

Анотація
Проаналізовано проблеми, пов'язані із захистом звукової інформації та запропоновано їх вирішення.
Ключові слова: безпека, технології, захист інформації.

Abstract
Problems related to the protection of audio information are analyzed and solutions are suggested.
Keywords: security, technology, protection of information.

Вступ

У наш час бурхливого розвитку техніки та економіки поняття "безпека" здобуває розширений зміст і містить у собі такі складові, як фізична, юридична й інформаційна безпека.

Особливе місце займає інформаційна безпека у зв'язку зі зростаючою роллю інформації в житті суспільства та вимагає до себе все більшої уваги. Успіх виробничої й підприємницької діяльності в чималому ступені залежить від уміння розпоряджатися таким найціннішим товаром, як інформація. Зараз головним ресурсом замість капіталу стає інформація. Інформаційні ресурси є об'єктами власності громадян, організацій, громадських об'єднань, держави.

Багатоваріантність побудови інформаційних систем дає багато рішень в сфері розробки систем захисту інформації. Широкомасштабне використання обчислювальної техніки і телекомунікаційних систем в рамках територіально розподіленої мережі, перехід на цій основі до безпаперової технології, збільшення об'ємів інформації, збільшення кількості користувачів приводить до того що необхідно збільшувати, покращувати рівень якості захисту інформації

У зв'язку з вищевикладеним, тематика даної роботи, присвяченої розв'язанню задачі захисту звукових файлів і телефонних переговорів, що здійснюються по цифрових лініях зв'язку, є актуальною.

Основний зміст

Суть проблеми, що виникла на сучасному етапі розвитку науки, техніки і технологій в галузі комунікацій - це забезпечення безпеки передавання інформації.

Це становище обумовлено тим, що в ми живемо в середовищі інформаційних технологій, куди перекочують всі соціальні проблеми людства, в тому числі і проблеми безпеки. Багатоваріантність побудови інформаційних систем дає багато рішень в сфері побудови систем захисту інформації. Широкомасштабне використання ОТ і телекомунікаційних систем в рамках територіально розподіленої мережі, перехід на цій основі до безпаперової технології, збільшення об'ємів інформації, збільшення кількості користувачів приводить до того що необхідно збільшувати, покращувати рівень якості захисту інформації.

Відомі рішення проблеми захисту звукової інформації, які існують на даний час уже неповністю задовольняють вимоги часу.

Порівнюючи рівні криптостійкості різних алгоритмів зрозуміло, що та програма яка має більший розмір ключа, має вищий рівень криптостійкості. Але при цьому виникає проблема: якщо ключ занадто великий, то його не можливо буде зберігати в пам'яті, отже прийдеться зберігати на носії інформації, який можуть викрасти, загубити тощо. Тому потрібно знайти альтернативний шлях захисту інформації від прослуховування зловмисником. Для вирішення цієї проблеми потрібно розробити програму яка використовуватиме цифровий криптографічний метод захисту інформації, а саме - метод однократного гамування, який теоретично не піддається розшифровці (зламу). Цей метод було модифіковано таким чином, що гама не є постійною. Гама залежить від паролю, який

задає правило вибору випадкових чисел з масиву. Масив випадкових чисел може коливатись в діапазоні від 2Мб-50Мб. Це не дає зловмиснику взнати точний розмір масиву, який використовується при гамуванні, що є значною перевагою. Довжина паролю 128 біт, тобто 16 байт.

Отже, цей метод має подвійний захист, оскільки для розшифрування звукового файлу зловмиснику потрібно мати конкретний масив випадкових чисел, який повинен зберігатись на носії інформації (флеш-карта, компакт-диск, жорсткий диск і т.п.), по-друге, потрібно знати пароль, який користувач просто пам'ятає.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

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

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

3. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с.

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

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

6. 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.

7. Глинчук Л.Я. Г 54 Криптологія: навч.-метод. посіб. / Людмила Ярославівна Глинчук – Луцьк: Вежа-Друк, 2014. – 164 с.

Ірина Леонідівна Медяна – студентка факультету менеджменту та інформаційних технологій, Вінницький національний технічний університет, Вінниця, e-mail:fm.ub16.mediana@gmail.com

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