

4. Krichen M, Ammi M, Mihoub A, Almutiq M. Blockchain for Modern Applications: A Survey. Sensors (Basel). 2022 Jul 14; 22(14): 5274. doi: 10.3390/s22145274. PMID: 35890953; PMCID: PMC9317832.
5. Топчій, М., & Гальчинський, Л. (2022). Підвищення рівня безпеки смарт-контрактів в мережі ethereum від шахрайства за рахунок використання реверсивних токенів. Collection of Scientific Papers «ΛΟΓΟΣ», (November 11, 2022; Paris, France), 71-77. <https://doi.org/10.36074/logos-11.11.2022.20>

**Гресь Олександр Володимирович,**  
кандидат технічних наук, асистент кафедри  
радіотехніки та інформаційної безпеки,  
Чернівецький національний університет  
імені Юрія Федьковича, м. Чернівці  
ORCID: 0000-0002-8465-193X

**Косован Василь Михайлович,**  
кандидат фізико-математичних наук,  
асистент кафедри математичного моделювання,  
Чернівецький національний університет  
імені Юрія Федьковича, м. Чернівці  
ORCID: 0009-0001-8628-3130

## **ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ КОМПЛЕКСУ ЗАХИСТУ АУДІОІНФОРМАЦІЇ**

Інтернет-адреса публікації на сайті:  
<http://www.konferenciaonline.org.ua/ua/article/id-1705/>

В даний час спостерігається зростання об'ємів аудіо та візуальної інформації, що передаються по мережах загального користування. Водночас збільшилася і кількість загроз та кіберінцидентів, внаслідок чого інформація, яка циркулює в інформаційних мережах загального користування стає легкою «здобичкою» для зловмисників [1].

Можливість несанкціонованого отримання та зміни інформації ставлять під загрозу її цілісність, конфіденційність і достовірність.

На сьогоднішній день забезпечення захисту інформації в мережах є актуальною задачею, для вирішення якої застосовують різні методи. Забезпечення захисту інформації, яка передається в інформаційних мережах, можливе шляхом її захисту за допомогою використання сучасних методів шифрування та апаратних засобів [1].

Всі існуючі засоби захисту інформації, яка передається по інформаційних мережах, можна розділити на програмні, апаратні та програмно-апаратні. Одним з недоліків програмних засобів захисту є можливість модифікування коду програми в разі його отримання зловмисником. Апаратні пристрої захисту в певній мірі позбавлені цього недоліку, оскільки зміна інформації, що

зберігається чи обробляється пристроєм можлива тільки у разі безпосереднього доступу зловмисника до пристрою. Тому найкращим варіантом забезпечення захисту інформації, є використання програмно-апаратних засобів [1, 2].

В даній роботі пропонується використання сучасних апаратних платформ для реалізації програмно-апаратного комплексу захисту аудіоінформації.

Запропонований пристрій включає блок апаратного шифрування та програмне забезпечення. Для реалізації апаратного ядра пристрою запропоновано використовувати сучасні програмовані плати (наприклад на базі STM32, ESP82XX та інші) [2, 3].

Програмна частина комплексу реалізована на мові C та забезпечує отримання аудіоданих від користувача, відправку та вивід даних користувачеві, забезпечує процедури маршрутизації аудіо та службової інформації. Апаратна частина виконує функції шифрування/розшифрування аудіоінформації та обчислення ключа шифрування. В якості методу шифрування інформації в даному комплексі можна застосувати алгоритм AES. Даний алгоритм має відносно просту внутрішню архітектуру, а отже його програмна реалізація займає малий об'єм пам'яті в апаратних пристроях.

Структурна схема запропонованого програмно-апаратного комплексу представлена на рис. 1.

Для запису аудіоінформації від користувача використовується стандартний аудіопристрій (мікрофон) та збереження даних в буфері. Далі, після отримання запиту на виконання, виконується операція шифрування / розшифрування, а необхідні для виконання даної операції дані надсилаються через USB-порт. У платах STM32 наявний апаратно реалізований інтерфейс USB 2.0 Full Speed, який працює на частоті 48 МГц та забезпечує максимальну швидкість обміну даними – 12 Мбіт/с. Також в даному апаратному рішенні існує підтримка низькорівневих операцій (наприклад прийом-передача пакетів, операції з CRC, маршрутизація пакетів).

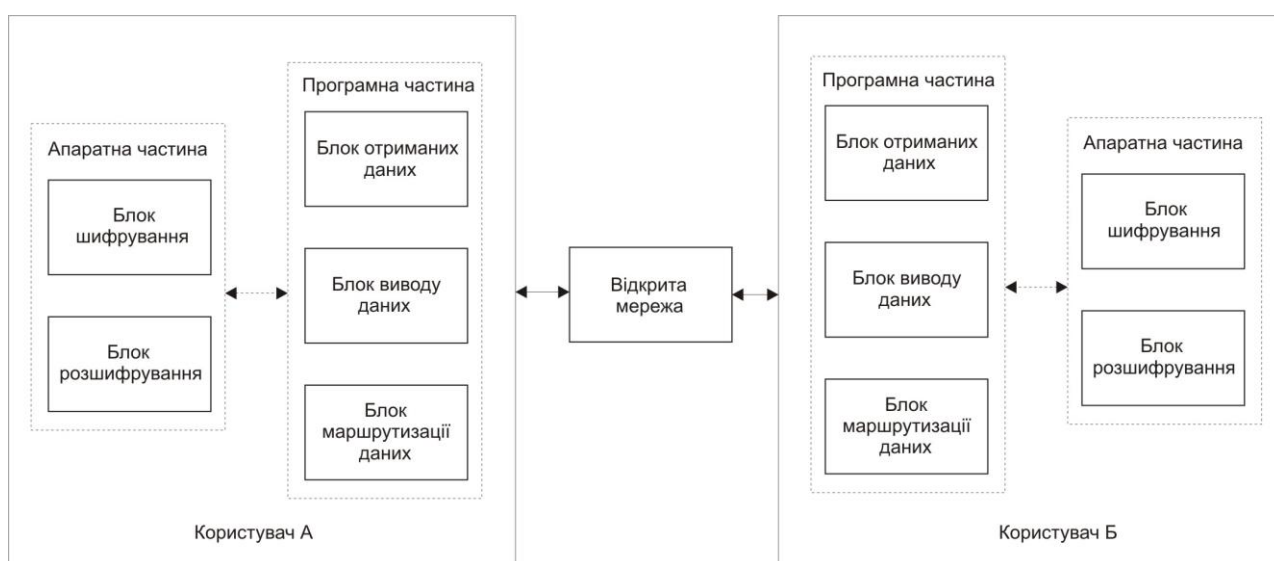


Рис. 1. Структурна схема програмно-апаратного комплексу захисту аудіоінформації

Передача та обмін зашифрованою аудіоінформацією між користувачами через відкриті канали зв'язку (мережі) реалізується за допомогою транспортного протоколу TCP.

Отже, запропонований комплекс забезпечує надійний захист аудіоінформації з використанням сучасних програмно-апаратних рішень та можливістю використання та модифікації існуючих методів шифрування. Інтерфейс розробленого програмного забезпечення містить всі необхідні опції для відтворення, запису, збереження аудіоінформації та має можливість задання та зміни адреси отримувача.

### **Література:**

1. Гресь О. В., Верига А. Д., Політанський Р. Л., Дробик О. В. Апаратна реалізація пристрою шифрування мовної інформації. *Сучасний захист інформації*. 2014. №3. С. 71-77.
2. XueFeng Cheng, HongMei Zhu, Juan Liu et al. A new hyperchaotic system with dynamical analysis and its application in image encryption based on STM32, 22 November 2023, PREPRINT (Version 1) available at Research Square [https://doi.org/10.21203/rs.3.rs-3637346/v1]
3. Ali M, Mallik A., Shahadat M. IoT Implemented Encryption Voice Transmission System with Particle Photon Microcontroller. *4th International Conference on Energy and Power (ICEP2022)*. MIST, Dhaka, Bangladesh.

*Дворянников Сергій Олександрович, студент,  
Чернівецький національний університет  
імені Юрія Федьковича, м. Чернівці*

*Сопронюк Тетяна Миколаївна, доцент,  
Чернівецький національний університет  
імені Юрія Федьковича, м. Чернівці  
ORCID: 0000-0002-7031-9880*

## **РОЗРОБКА САЙТУ ДЛЯ МОНІТОРИНГУ КРИПТОВАЛЮТНОГО РИНКУ**

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1684/>

Криптовалюта [1] – це децентралізовані цифрові гроші, призначені для використання в Інтернеті. Біткойн, який був створений у 2008 році, був першою криптовалютою, і досі залишається найбільшим, найвпливовішим та найвідомішим. Протягом десяти років з того часу Біткойн та інші криптовалюти, такі як Ефіріум, зростали як цифрові альтернативи грошам, виданим урядами.

Освоєння ринку криптовалют – це завдання, що набуває все більшої актуальності в сучасному фінансовому світі. За останнє десятиліття