УДК 004.056.5:004.934
DOI: 10.31673/2409-7292.2025.026026

Юрх Н.Г., Петченко М.В., Іванченко І.С.

АНАЛІЗ МЕТОДІВ ЗАХИСТУ СИСТЕМИ ПЕРЕДАВАННЯ МОВНОЇ ІНФОРМАЦІЇ

У статті розглянуто сучасні підходи до захисту систем передавання мовної інформації в умовах зростаючих кіберзагроз, особливо в контексті гібридної війни та дій правового режиму воєнного стану. Акцент зроблено на важливості забезпечення конфіденційності, цілісності та доступності мовного контенту, що передається через дротові та бездротові канали зв'язку в цивільному та військовому секторі. Проведено аналіз класичних і сучасних методів захисту, включно з криптографічними (AES, RSA, ECC), стеганографічними, адаптивними та організаційно-технічними засобами. Обґрунтовано доцільність використання протоколів SRTP, ZRTP, а також технологій динамічного керування ключами, систем виявлення вторгнень (IDS) та методів акустичного і вібраційного екранування. Показано, що ефективність захисту значно зростає при поєднанні кількох рівнів безпеки та адаптації до умов зовнішнього середовища. У статті представлено порівняльну таблицю оцінювання методів. Висновки підкріплено даними з вітчизняних і зарубіжних наукових публікацій, що дозволяє визначити перспективні напрями розвитку систем захисту мовної інформації.

Ключові слова: захист інформації; мовна інформація; стеганографія; криптографія; адаптивні методи; системи зв'язку; безпека передачі мовної інформації.

Вступ

У сучасних умовах стрімкого розвитку цифрових технологій та зростання обсягів передавання інформації системи захищеного мовного зв'язку набувають визначального значення як у цивільному, так і у військовому секторах. Особливої актуальності питання захисту мовної інформації набуває в умовах гібридних загроз, широкого застосування засобів радіоелектронної боротьби (РЕБ) і кібератак з боку противників, зокрема у ході збройної агресії рф проти України.

Системи передавання мовної інформації (СПМІ) є критичними компонентами комунікаційної інфраструктури, через які передається оперативна, стратегічна та конфіденційна інформація. Будь-яка вразливість у таких системах може бути використана противником для прослуховування переговорів, перехоплення даних, порушення автентичності повідомлень або впливу на процеси ухвалення рішень у режимі реального часу.

Дані ризики вимагають впровадження сучасних і ефективних методів захисту, які враховують специфіку мовних сигналів, мережевих протоколів та контексту функціонування інформаційних систем у бойових і кризових умовах. У зв'язку з цим, метою даного дослідження є комплексний аналіз існуючих методів захисту мовної інформації під час її передавання, а також критична оцінка їх придатності для застосування у високоризикових сценаріях, таких як військовий зв'язок, канали спецзв'язку та інфраструктура критичної інформаційної безпеки.

Результати дослідження дозволяють окреслити сучасні технологічні тенденції, визначити переваги та обмеження застосування конкретних методів, а також сформулювати рекомендації щодо підвищення стійкості СПМІ до зовнішніх загроз.

Метою даної статті є аналіз сучасних методів захисту мовної інформації при її передаванні, з урахуванням практичної ефективності, технологічної складності та можливості адаптації до змінного середовища передавання. Стаття також спрямована на порівняння методів з урахуванням актуального наукового доробку та практичних впроваджень.

Огляд літератури та аналіз існуючих методів та моделей

Мовний сигнал – це складний акустичний феномен, який включає в себе змінні параметри тиску в повітряному середовищі, що кодують змістовне навантаження мовного повідомлення. Ці коливання мають енергетичний спектр, здебільшого зосереджений у діапазоні частот 300-4000 Гц, і виникають у результаті генерації хвиль стиснення та розрідження у повітрі під впливом роботи голосового апарату людини.

Під впливом звукових хвиль можуть виникати вібраційні резонанси в огороджувальних конструкціях будівель і в інженерних комунікаціях приміщень, у яких присутнє джерело мовного сигналу. У результаті цього первинний акустичний сигнал може перетворюватися у вторинні джерела випромінювання, які створюються шляхом взаємодії з різними елементами середовища. Такими вторинними перетворювачами можуть бути: гучномовці, мікрофони, телефони, акселерометри тощо.

Для забезпечення процесу передавання мовної інформації в сучасних умовах переважно застосовуються різноманітні радіотехнічні засоби, що інтегруються в цілісні системи, зокрема супутникові, стільникові, телефонні тощо. Система передавання інформації (СПІ) визначається як сукупність взаємопов'язаних технічних засобів, організованих у єдиний технологічний ланцюг, що функціонує на основі спільного фізичного принципу генерації, обробки та передавання сигналів з чітко визначеними правилами взаємодії її елементів.

До основних складових будь-якої СПІ належать: передавальний пристрій (передавач), приймальний пристрій (приймач) і канал зв'язку, або лінія зв'язку (ЛЗ). Передавальні та приймальні елементи представлені технічними пристроями, здатними формувати електричні сигнали, здійснювати їхню модуляцію, обробку та передачу до відповідного абонента. Лінія зв'язку, у свою чергу, охоплює як фізичне середовище поширення сигналу, так і допоміжні технічні засоби, що забезпечують стабільну та безперебійну передачу даних.

Усі компоненти – від передавача до приймача разом із середовищем розповсюдження сигналів – утворюють функціонально завершену структуру, яка в телекомунікаціях визначається як канал зв'язку. Останній трактується як система технічних засобів, що забезпечує передачу повідомлень між джерелом інформації та її одержувачем. У вузькому сенсі канал зв'язку це лише фізичне середовище, яке забезпечує передачу сигналів.

Канали зв'язку класифікуються за різними критеріями: типом передаваних повідомлень, природою сигналів, напрямом передавання, конфігурацією лінії зв'язку, рівнем застосування криптографічного захисту тощо. За типом середовища поширення сигналів канали передавання поділяються на механічні, акустичні, оптичні та електричні. Останні два – електричні та оптичні – можуть реалізовуватись як дротовими, так і бездротовими засобами, що за певних умов формують природні шляхи потенційного витоку інформації. У таких каналах передається мовна інформація, попередньо перетворена відповідно до характеристик каналу.

Захист мовної інформації становить сукупність організаційних і технічних заходів, спрямованих на попередження витоку інформації, що передається у вигляді акустичних сигналів, які формуються голосовим апаратом людини. У загальному випадку така інформація належить до категорії мовної, якщо вона існує у формі звукових коливань, що продукуються природними фізіологічними механізмами мовлення. У контексті інформаційної безпеки особливу загрозу становлять технічні канали витоку мовної інформації (ТКВІ), що виникають внаслідок можливості перехоплення мовного сигналу через різні типи середовищ та пристроїв. Залежно від природи сигналу та способів його перехоплення, ТКВІ класифікуються на:

- акустичні канали – базуються на поширенні звукових хвиль у повітряному середовищі, особливо у випадках відкритих дверей, вікон або вентиляційних отворів;
- віброакустичні канали – формуються внаслідок проникнення звукових коливань у будівельні конструкції (стіни, стелі, підлоги, вікна) та комунікації (трубопроводи, системи кондиціювання), що викликає механічні вібрації;
- оптико-електронні канали – використовують лазерне зондування з подальшою демодуляцією сигналів, які відбиваються від вібруючих під дією мовного сигналу поверхонь (вікна, дзеркала);
- акустоелектричні канали – виникають внаслідок впливу звукових хвиль на електронні компоненти (ємності, індуктивності), що призводить до модуляції струмів через мікрофонний ефект або електромагнітне нав'язування;

- параметричні канали – формуються при паразитній модуляції електромагнітних випромінювань пристроїв (наприклад, гетеродинів радіоприймачів або телевізорів), що реагують на акустичний вплив у межах приміщення;
- канали через закладні пристрої – пов'язані з використанням спеціально розміщених технічних засобів збору інформації, призначених для несанкціонованого зняття мовних або візуальних даних.

Сучасні дослідження в галузі захисту мовної інформації при передаванні фокусуються на забезпеченні цілісності, конфіденційності та автентичності даних. В умовах гібридної війни, яку веде рф проти України, ці питання набувають критичної актуальності. В наукових працях Stallings W. [1], Schneier B [2], Koblitz N. [3] висвітлюються криптографічні методи захисту, зокрема використання алгоритмів симетричного й асиметричного шифрування. Особливу увагу також приділено стеганографії Johnson N.F., Duric Z., Jajodia S. [4], а також захисту каналів передавання мовної інформації в мобільних мережах Sklavos N., Zhang X. [5]. Дослідження вітчизняних учених, таких як Кузнецов О.О., Євсеєв С.П., Король О.Г. [6], акцентують на застосуванні адаптивних алгоритмів шифрування.

Криптографічні методи захисту мовної інформації

Криптографічний захист виступає одним із базових інструментів забезпечення конфіденційності мовної інформації, особливо в умовах функціонування систем цифрового зв'язку, зокрема VoIP. Сучасні засоби захисту застосовують поєднання симетричних та асиметричних криптоалгоритмів. Симетричне шифрування, зокрема алгоритм AES (Advanced Encryption Standard), демонструє високу ефективність при шифруванні мовного потоку в реальному часі завдяки низькому рівню обчислювальних витрат та швидкодії. Натомість асиметричні алгоритми, такі як RSA (Rivest–Shamir–Adleman) та ECC (Elliptic Curve Cryptography), доцільно використовуються для безпечного обміну ключами між комунікантами, особливо в умовах відкритих каналів зв'язку [1,].

З метою захисту голосових даних у мережах передачі в реальному часі (RTP) активно використовуються протоколи шифрування, зокрема SRTP (Secure Real-time Transport Protocol) та ZRTP. Протокол SRTP забезпечує конфіденційність, автентичність та цілісність мовного трафіку, використовуючи симетричні ключі для шифрування та HMAC для перевірки даних [7]. У свою чергу, ZRTP передбачає обмін ключами шифрування без використання централізованої інфраструктури, використовуючи дифі-гелманівський протокол через аудіоканал [8].

Окрему увагу наукова спільнота приділяє застосуванню хаотичних систем для генерації ключів шифрування. Такі системи, які базуються на теорії динамічного хаосу, демонструють перспективи у формуванні стійких псевдовипадкових послідовностей, що можуть бути використані для посилення криптографічних методів захисту мовної інформації. Проте, слід зазначити, що зазначений підхід поки що перебуває на стадії активного наукового дослідження і не має широкого впровадження в стандартизованих протоколах.

Стеганографічні методи захисту мовної інформації

У контексті забезпечення інформаційної безпеки мовних даних стеганографічні методи набувають все більшої актуальності, особливо в умовах гібридних загроз. На відміну від криптографічних підходів, що зосереджені на перетворенні вмісту повідомлення, стеганографія орієнтується на приховування факту передавання конфіденційної інформації шляхом її інтеграції у сторонні мультимедійні носії, зокрема аудіо- та відеопотоки. Зазначений метод створює додатковий рівень захисту, унеможливлюючи ідентифікацію самого факту передачі захищених даних при перехопленні каналу зв'язку. Проте ефективність стеганографії значною мірою залежить від типу використаного носія, а також від рівня стійкості обраного алгоритму до виявлення або дестеганалізу [9]. Загалом, сучасні дослідження демонструють перспективність використання методів спектрального зміщення, модуляції фази та імпульсної модуляції, що забезпечують високий рівень інтеграції повідомлення при мінімальному впливі

на якість сигналу [10]. Разом із цим, необхідно враховувати ризики, пов’язані із застосуванням автоматизованих засобів виявлення стеганографічного впливу, зокрема на основі нейронних мереж, що використовуються для стеганографічного аналізу.

Адаптивні методи захисту мовної інформації

У сучасних системах передавання мовної інформації, особливо в умовах зростання обсягів мобільного трафіку, важливу роль відіграють адаптивні методи захисту, які забезпечують динамічне налаштування параметрів безпеки відповідно до змін середовища функціонування. Зокрема, ці методи реалізують зміну алгоритмів шифрування, швидкості або частоти передавання сигналу, вибір протоколів зв’язку тощо. Такий підхід дозволяє мінімізувати ризики несанкціонованого доступу та забезпечити безперервність захисту навіть у нестабільних або ворожих інформаційних умовах.

Адаптивність досягається шляхом інтеграції механізмів аналізу ситуації в реальному часі, що дозволяє виявляти зміну загроз або спроби атак і відповідно коригувати параметри безпеки. Наприклад, у разі виявлення спроби перехоплення трафіку система може миттєво змінити криптографічний алгоритм з AES на більш стійкий варіант або активувати додаткові рівні захисту, включаючи багаторівневу автентифікацію.

У сфері військових комунікацій подібні методи дозволяють забезпечити високий рівень мобільності та стійкості до радіоелектронного впливу противника. Відповідно до досліджень, адаптивні системи демонструють вищу ефективність при функціонуванні в умовах наявності перешкод, глушіння, динамічної зміни мережевої інфраструктури [11].

Крім того, в умовах гібридної війни, яка актуальна для України, адаптивні методи захисту мовної інформації мають вирішальне значення, оскільки дозволяють забезпечити гнучкість захисних механізмів, включаючи можливість віддаленого оновлення політик безпеки, інтелектуальну маршрутизацію повідомлень та застосування процедур контекстного шифрування.

Таким чином, використання адаптивних методів захисту є перспективним напрямом розвитку інформаційної безпеки мовних комунікацій, що поєднує високий рівень стійкості до загроз з ефективною реакцією на нові ризики.

Організаційні та технічні заходи захисту мовної інформації

Забезпечення ефективного захисту мовної інформації в сучасних умовах вимагає впровадження як організаційних, так і технічних заходів. Організаційні заходи відіграють ключову роль у створенні системного підходу до безпеки, формуючи нормативно-правове середовище, яке регулює діяльність персоналу щодо поводження з конфіденційною інформацією. Зокрема, політика інформаційної безпеки повинна включати регламентацію доступу до мовної інформації, проведення інструктажів, підвищення рівня обізнаності працівників щодо потенційних загроз та механізмів їх усунення [12].

Серед організаційних заходів особливе значення має класифікація приміщень за рівнем захищеності від витоку акустичної інформації, а також організація фізичного захисту об'єктів інформаційної діяльності. Досвід українських органів безпеки засвідчує ефективність реалізації багатоетапних програм захисту, які включають обов'язковий контроль доступу та застосування принципу найменших привілеїв.

До технічних заходів належать впровадження спеціалізованих технічних засобів захисту, серед яких: екранування приміщень, використання засобів активного шумозаглушення, впровадження систем контролю і виявлення технічних засобів несанкціонованого знімання інформації, зокрема акустичних та вібраційних каналів.

Крім того засоби захисту за активністю поділяються на пасивні, напівактивні і активні. Найбільш ефективними і широко застосовуваними є активні методи [13, 14, 15].

До засобів пасивного захисту відносяться фільтри та інші пристрої для мережі спільного користування (МСК). В останній час почали застосовувати управління маршрутами. Воно призначене для організації передачі інформації в МСК тільки по маршрутах, які утворилися

за допомогою надійних та безпечних технічних засобів і систем. При цьому організовується контроль з боку одержувача, який у випадку виникнення підозри про компрометацію використовуваної системи може змінити маршрут проходження даних.

Недоліком засобів пасивного захисту є те, що вони не забезпечують захист від активних засобів нападу і частково не від всіх пасивних засобів нападу.

Відомо, що основними каналами передачі інформації в СПМІ є лінії зв'язку (телефонні). Захист ліній зв'язку являє собою дуже серйозну проблему, оскільки ці лінії частіше всього називаються безконтрольними і з них можуть несанкціоновано отримати інформацію [16].

Найбільш прогресивним методом захисту на сьогоднішній день є активні засоби захисту. Досягається це шляхом подачі в лінію додаткових сигналів (загороджувальної перешкоди) і зміни стандартних параметрів телефонної лінії (зазвичай в розумних межах змінюється складова напруги в лінії і струм в ній) у всіх режимах роботи.

Для того щоб перешкоди не дуже сильно заважали передачі інформації, вони компенсуються перед подачею на приймальну апаратуру. Щоб уникнути незручності для віддаленого абонента перешкоди підбираються з сигналів, які затухають в процесі проходження по лінії або легко фільтруються абонентськими комплектами апаратури. Для якісного впливу перешкоди на апаратуру перехоплення її рівень зазвичай в кілька разів, а іноді і на порядок перевершує рівень сигналу, що передається в лінії.

З точки зору організації застосування системи активного захисту (САЗ) підрозділяються на індивідуальні (здійснюють придушення одного або декількох інформаційних сигналів, що випромінюються окремим передавальним об'єктом) і колективні (здійснюють придушення небезпечних сигналів декількох передавальних об'єктів).

Методи створення перешкод реалізуються шляхом застосування вузькосмугових генераторів шуму (ГШ), багатофункціональних комплексів придушення, генераторів синусоїдальних перешкод і широкосмугових ГШ.

Вузькополосні ГШ створюють прицільні маскуючі перешкоди на одній або декількох фіксованих частотах. Рівень потужності, яка ними випромінюється, повинен бути співмірний з вихідною потужністю сигналу, що передається. Спектральний склад перешкоди повинен покривати за граничними частотами інформаційний сигнал.

У багатофункціональних комплексах придушення застосовуються прицільні перешкоди, які створювані вузькосмуговими ГШ.

Широкосмугові ГШ знаходять широке застосування в задачах маскування засобів обчислювальної техніки. Однак застосування широкосмугових ГШ дає позитивний ефект тільки в ряді окремих випадків: наявність апріорних даних про місцезнаходження передавальної і приймаючої сторін; застосування сигналів з потужністю, яка знижує до середнього рівня шумів лінії з метою їх маскування.

Генератори спеціальних перешкод поки не знайшли широкого практичного і самостійного застосування в цілях захисту. Перехід до інших, енергетично більш вигідним видам перешкод, дозволяє підвищити ефективність захисту і застосування САЗ.

Завдання створення САЗ на базі генераторів спеціальних перешкод вивчені недостатньо. Розробка ефективних методів захисту безпосередньо базується на принципах проектування і оцінки систем захисту інформації.

Крім того, доцільним є застосування сертифікованих засобів захищеного зв'язку, які відповідають вимогам державної системи технічного захисту інформації [17].

Інтегроване застосування різних методів захисту мовної інформації та організаційних і технічних заходів безпеки забезпечує формування багаторівневої моделі захисту мовної інформації. Така модель базується на принципах розмежування доступу, мінімізації ризиків технічного прослуховування та забезпечення постійного моніторингу інформаційного середовища. Це дозволяє ефективно протидіяти витоку мовної інформації, що циркулює у службових приміщеннях, зокрема в адміністративних будівлях органів державної влади,

об’єктах критичної інфраструктури, енергетичних системах, засобах зв’язку та на стратегічних об’єктах оборонного призначення. Реалізація такого комплексу заходів сприяє зниженню ймовірності несанкціонованого доступу до конфіденційних аудіоданих та підвищує загальну стійкість об'єкта до сучасних технічних загроз.

Таблиця 1

Порівняльна таблиця методів захисту мовної інформації

Метод захисту		**Переваги**	**Недоліки**	**Сфери застосування**
Криптографічні методи	симетричне шифрування (AES)	висока швидкість шифрування, ефективність у закритих мережах	необхідність безпечного обміну ключами	закриті мережі, військовий зв'язок
	асиметричне шифрування (RSA, ECC)	безпечний обмін ключами через відкриті канали	низька продуктивність при обробці великих обсягів	гібридні системи, спецзв’язок
Стеганографічні методи		приховування факту передачі конфіденційної інформації	залежність від носія і вразливість до стеганалізу	мультимедійні передачі, прихована комунікація
Адаптивні методи		гнучкість до умов середовища, підвищена стійкість до атак	складність реалізації, потреба в динамічному аналізі	мобільні системи, змінне середовище
Організаційні заходи		формування культури безпеки, регламентування доступу	не гарантують технічного захисту самостійно	державні установи, критична інфраструктура (КІ)
Технічні заходи		фізичний захист каналів, виявлення закладних пристроїв	необхідність постійного оновлення і контролю	приміщення з КІ, офіси спецслужб

Висновки

У процесі дослідження було здійснено комплексний аналіз сучасних методів захисту мовної інформації під час її передавання в умовах зростаючих кіберзагроз, гібридної війни та інформаційної боротьби. Визначено, що найбільш ефективним підходом є поєднання кількох рівнів захисту, що включають криптографічні, стеганографічні, адаптивні методи, організаційні та технічні заходи. Зокрема, протоколи SRTP та ZRTP, а також сучасні системи генерації ключів на основі хаотичних функцій демонструють високу ефективність у забезпеченні конфіденційності та автентичності мовного контенту.

Встановлено, що адаптивні методи дозволяють гнучко реагувати на зміну умов середовища та типи атак, що забезпечує додаткову стійкість у мобільних або ворожих умовах. Стеганографічні підходи підвищують рівень захисту за рахунок приховування факту передавання інформації, що ускладнює її виявлення та перехоплення. Технічні заходи, зокрема активні методи екранування та шумозаглушення, суттєво знижують ймовірність витоку мовної інформації через технічні канали. Організаційні заходи, такі як регламентування доступу, навчання персоналу та застосування принципу найменших привілеїв, створюють додатковий рівень контролю над обробкою конфіденційної інформації.

Проведений аналіз підтверджує, що у сучасних умовах доцільним є впровадження багаторівневих систем захисту, які поєднують як традиційні, так і інноваційні підходи. Застосування таких систем дозволить ефективно протидіяти загрозам витоку мовної інформації в умовах воєнного стану та кібератак. Подальші дослідження мають бути

зосереджені на розробці інтелектуальних систем адаптації захисту, а також стандартизації ефективних методик для оцінки захищеності каналів передавання мовної інформації.

Перелік посилань

1. Stallings W. (2020). Cryptography and Network Security: Principles and Practice. https://mrce.in/ebooks/Cryptography%20&%20Network%20Security%208th%20Ed.pdf.

2. Schneier B. (2020). Applied Cryptography.

3. Koblitz N. (1994). A Course in Number Theory and Cryptography https: // doi.org /10.1007/978-1-4419-85927.

4. Johnson N.F., Duric Z., Jajodia S. (2001). Information Hiding. https://doi.org/10.1007/978-1-4615-4375-6.

5. Sklavos N., Zhang X. (2007). Wireless Security and Cryptography. https://doi.org/10.1201/9780849387692.

6. Кузнецов О.О., Євсеєв С.П., Король О.Г. Захист інформації в інформаційних системах. Методи традиційної криптографії. Х.: Вид. ХНЕУ, 2010. 316 с.

7. Baugher M., McGrew D., Naslund M., Carrara E., Norrman K. The Secure Real-time Transport Protocol (SRTP). RFC 3711. Internet Engineering Task Force, 2004. 54 p.

8. Zimmermann P., Johnston A., Callas J. ZRTP: Media Path Key Agreement for Unicast Secure RTP. RFC 6189. IETF, 2011. 84 p.

9. Хорошко В. О. Основи комп'ютерної стеганографії : навч. пос. / В.О. Хорошко, В.О. Азаров В.О., М. Є. Шелест. Вінниця : ВДТУ, 2003. 143 с.

10. Johnson, N. F., & Katzenbeisser, S. A survey of steganographic techniques / N. F. Johnson, S. Katzenbeisser // Information Hiding: Techniques for Steganography and Digital Watermarking. Boston: Artech House, 2016. P. 43–78.

11. Леонов, М. В. Використання адаптивних засобів захисту в мобільних системах зв'язку / М. В. Леонов // Наука і оборона. 2022. №1. С. 56-62.

12. Стратегія кібербезпеки України: Указ Президента України від 26.08.2021 № 447/2021. https://www.president.gov.ua/documents/4472021-40013.

13. Домарев В.В. Безпека інформаційних технологій. Системний підхід. Київ: ТИД «ДС», 2004. 992 с.

14. Хорошко В.А., Чекатков А.А. Методи і засоби захисту інформації. Київ: Юниор, 2003. 501 с.

15. Домарєв В.В. Сучасні методичні та організаційні підходи до захисту інформації. Збірник наукових статей ХНЕУ. Харків, 2008. С. 17-18.

16. Хома В.В. Методи та засоби забезпечення конфіденційності телефонних повідомлень. Сучасна спеціальна техніка Київ, 2009. №3(18). С. 50-59.

17. Засоби ТЗІ, які мають експертний висновок про відповідність вимогам технічного захисту інформації. https://cip.gov.ua/ua/news/zasobi-tzi-yaki-mayut-ekspertnii-visnovok-pro-vidpovidnist-do-vimog-tekhnichnogo-zakhistu-informaciyi.

Надійшла 14.05.2025