# КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ / CYBERSECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

**DOI: 10.18372/2225-5036.28.16949**

# ПОРІВНЯЛЬНИЙ АНАЛІЗ МАТЕМАТИЧНИХ МОДЕЛЕЙ МОВНОЇ ІНФОРМАЦІЇ

**Олександр Корченко[1,2], Ольга Грищук[3]**

*[1]Національний авіаційний університет, Україна*
*[2]Університет у Бєльсько-Бялій, Польща*
*[3]Житомирський військовий інститут імені С.П. Корольова, Україна*

**КОРЧЕНКО Олександр Григорович,** д.т.н., професор,
Засл. діяч науки і техн. України, лауреат Державної премії України в галузі наук. і техн.
*Рік та місце народження:* 1961 рік, м. Київ, Україна.
*Освіта:* Київський інститут інженерів цивільної авіації (з 2000 року – Національний авіаційний університет), 1983 рік.
*Посада:* завідувач кафедри безпеки інформаційних технологій з 2004 року;
візит-професор (Університет в Бєльсько-Бялій, Польща).
*Наукові інтереси:* кібербезпека.
*Публікації:* понад 360 друкованих публікацій, серед яких монографії, словники, підручники, навчальні посібники, наукові статті та патенти на винаходи.
*E-mail:* icaocentre@nau.edu.ua.
*ORCID ID: 0000-0003-3376-0631.*

**ГРИЩУК Ольга Михайлівна**
*Рік та місце народження:* 1984 рік, м. Житомир, Україна.
*Освіта:* Національний авіаційний університет, 2009 рік.
*Посада:* науковий співробітник науково-дослідного відділу інформаційної та кібернетичної безпеки з 2022 року.
*Наукові інтереси:* кібербезпека.
*Публікації:* 3 наукові статті, тези 7 доповідей.
*E-mail:* Ol.Hry@i.ua.
*ORCID ID: 0000-0001-6957-4748.*

***Анотація.*** *Загострення кібербезпекової ситуації навколо України потребує кардинального перегляду чинних підходів до забезпечення кібербезпеки інформаційно-комунікаційних систем держави. Випереджальні темпи розвитку засобів та технологій кібернападу обумовлюють необхідність пошуку нових нетривіальних (асиметричних) та одночасно практичних ідей, спрямованих на забезпечення кіберзахисту інформації незалежно від виду її подання. Останнім часом мовна інформація, яка циркулює в IP-мережах, стає об'єктом кібернападу з боку недобросовісних конкурентів, іноземних державних інституцій і просто зацікавлених осіб. Як відомо, одним із найдієвіших заходів кіберзахисту мовної інформації є її криптографічний захист. Відомі міжнародні та національні криптографічні протоколи забезпечують достатню криптографічну стійкість, але попри це кількість кіберзагроз мовній інформації не зменшується, а ,навпаки, збільшується пропорційно до зростання її цінності. Тому й надалі залишається актуальним питання підвищення рівня захищеності мовної інформації, яка циркулює в IP-мережах. Одним із перших етапів на шляху створення новітніх криптографічних засобів захисту мовної інформації є аналіз відповідних математичних моделей. Для встановлення переваг та недоліків відомих математичних моделей мовної інформації та вибору серед них за однакової точності тієї, яка враховуватиме індивідуальні особливості джерела мовної інформації, а також матиме прийнятну реалізованість для заданої системи параметрів, у статті наведено результати аналізу двох класів моделей: динамічних та стохастичних. Показано, що основними динамічними моделями мовної інформації, які належать до моделей першого класу, є вейвлет-моделі, імпульсно-модульовані та хвильові, моделі лінійного передбачення, гармонічні математичні моделі. У статі окрім відомих математичних моделей першого класу проаналізовано їх новий тип – фредгольмові моделі мовної інформації. До другого класу моделей, розглянутих у статті, включено два типи з найбільш поширених, а саме: акусто-фонетичні моделі та моделі мовного трафіка. Для кожної з досліджених моделей того чи іншого класу і типу було встановлено розробників, наведено*

*математичний апарат, який покладено в їх основу, формалізовано досліджувану математичну модель мовної інформації. На основі введеної якісної шкали за сукупністю визначених переваг та недоліків проаналізованих моделей оцінено ступінь досяжності одержаних результатів відповідно до поставленої в статті мети. Отже, проведений аналіз охопив найбільш поширені класи математичних моделей мовної інформації та дозволив серед них обрати ту, яка стане підґрунтям для розроблення новітніх криптографічних засобів захисту.*

***Ключові слова:*** *математична модель, мовна інформація, порівняльний аналіз, кібербезпека, IP-мережа, VoIP-телефонія, криптографічна атака, криптографічний захист.*

**Постановка проблеми**

Захист національних інтересів в інформаційній сфері [1] будь-якої розвиненої в технологічному та економічному плані держави безпосередньо пов'язаний із кіберзахистом [2] електронних інформаційних ресурсів її громадян, суспільства і державних інститутів [3]. Передусім заходи кіберзахисту передбачають криптографічний захист інформації в інтересах сил оборони сектора безпеки й оборони України під час управління державою в умовах надзвичайного стану та в особливий період [4]. Особлива роль у згаданих управлінських процесах відводиться криптографічному захисту мовної інформації, яка передається IP-мережами. Зростаюча одночасно кількість та складність криптографічних атак на мовну інформацію, яка передається в IP-мережах у світі в цілому [5]–[7] та в Україні зокрема [8], ставить під загрозу безпеку IP-мереж, які використовують для передачі мовної інформації. У свою чергу, ситуація, що склалася, спонукає до пошуку нових нетривіальних підходів до забезпечення їх кібербезпеки.

**Аналіз останніх досліджень**

Виходячи з фізичної сутності мовної інформації, з [9] та інших публікацій встановлено, що під згаданим терміном розуміється мовний сигнал аналогової природи, який, перетворюючись в аналого-цифровому пристрої, набуває дискретної форми й після подальшого оброблення описується одним із загальноприйнятих протоколів, на базі яких функціонують сервіси VoIP телефонії [9], [10]. При цьому аналогова природа мовного сигналу є визначальною для побудови його моделі, адже вибір тієї чи іншої математичної моделі мовної інформації в підсумку встановлюватиме підходи до побудови відповідних засобів її криптографічного захисту [12 -15].

Слід зазначити, що є й інші, відмінні від [9], підходи до формалізованого опису математичних моделей мовної інформації [16]–[19]. Таким чином, на підставі аналізу останніх досліджень і публікацій за темою дослідження встановлено, що на сьогодні вже розроблено достатньо велику кількість математичних моделей мовної інформації. Але цільові криптографічні атаки, спрямовані на порушення конфіденційності мовної інформації в IP-мережах [5] (*MITM*, *NAT Attack*), її цілісності (*Virus attack*, *NAT Attack)* та доступності (*Denial of Service Attacks, Virus attack, Toll Fraud attack*, *DHCP attack* та *Flooding attack*), а також на загрози безпеці інформації VoIP-трафіка загального характеру, порушення конфіденційності [6] (*Eavesdropping Unauthorized access*, *ID Spoofing*) та цілісності (*Caller ID, Call Redirection or Hijacking*), суттєво обмежують застосування на практиці відомих засобів криптографічного захисту мовної інформації. Отже, проведення порівняльного аналізу математичних моделей мовної інформації, які можуть бути використані для побудови перспективних апаратних та програмних засобів криптографічного захисту мовної інформації в IP-мережах, – це актуальне наукове та прикладне завдання.

**Метою дослідження є** встановлення переваг та недоліків відомих математичних моделей мовної інформації для вибору серед них за однакової точності такої, яка враховуватиме індивідуальні особливості джерела мовної інформації, а також матиме прийнятну реалізованість для заданої системи параметрів моделі.

**Виклад основного матеріалу дослідження**

З урахуванням наявних класифікацій моделей мовних сигналів [16], [20]–[25] та інших публікацій, доступних з відкритого друку, встановлено, що більшість із моделей можуть бути віднесені до двох основних класів: 1-й клас – це динамічні моделі мовної інформації; 2-й клас – стохастичні моделі мовної інформації.

*Моделі 1-го класу* є функціональними залежностями, у яких параметри змінюються в часі. На практиці з динамічних моделей мовної інформації найбільшого поширення набули математичні моделі, в основу яких, як показано в [26], покладено: вейвлет-коефіцієнти; імпульсно-модульовані сигнали; хвильові рівняння; метод лінійного передбачення; гармонічні математичні моделі. На основі відомих публікацій [18] та [27]–[30] запропоновано розширити коло наведених вище динамічних моделей мовної інформації, доповнивши їх математичною моделлю на основі інтегральних рівнянь Фредгольма першого роду.

*Моделі 2-го класу* – це стохастичні моделі, серед них найбільш поширеними є приховані марковські моделі [31]–[34] та стохастичні моделі на основі "on/off" послідовностей [35], [36]. Параметри моделей даного класу визначають на основі оброблення та аналізу статистичної інформації про мовну інформацію. У формалізованому вигляді їх описують параметричною залежністю, яка, як правило, має нестаціонарний характер.

Зважаючи на різну природу математичних моделей 1- го та 2- го класу, встановлення їх переваг та недоліків потребує більш ґрунтовного дослідження, суть та результати якого наведено нижче.

*Результати аналізу математичних моделей мовної інформації 1-го класу*

*Вейвлет-моделі мовної інформації.* Для побудови математичних вейвлет-моделей мовної інформації враховуються квазістаціонарні та стаціонарні ділянки мовного сигналу, які характеризуються нелінійними флуктуаціями різного масштабу [37]–[39]. Таке припущення дозволяє подати вейвлет-розкладання мовного сигналу $s(t)$ у вигляді суми з $N$ відліків [38]:

$$s(t)=\sum_{k=0}^{N/2^n-1} s_{nk}\varphi_{nk}+\sum_{j=1}^{N}\sum_{k=0}^{N/2^n-1} d_{jk}\psi_{jk};$$

$$\varphi_{nk}=2^{j/2}\varphi\left(2^j t-k\right), \text{де } j,k\in\mathbb{Z}; \quad (1)$$

$$\psi_{jk}=2^{j/2}\psi\left(2^j t-k\right), \text{де } j,k\in\mathbb{Z},$$

де $n$ – кількість рівнів декомпозиції моделі; $s_{nk}, d_{jk}$ – коефіцієнти апроксимації та деталізації вейвлет-розкладу; $\varphi$ – скейлінг (масштабна) функція; $\psi$ – базисний ("материнський") вейвлет.

У різних частотних діапазонах кількість рівнів декомпозиції моделі (1) варіює [39]. Наприклад, у [38] показано, що в частотному діапазоні Добеші-16 від 125 Гц до 4000 Гц вейвлет-модель мовної інформації (1) включає п'ять рівнів декомпозиції, а в частотному діапазоні Мейєра від 86 Гц до 5512 Гц – шість рівнів. Перевагою моделі (1) над іншими відомими динамічними моделями є можливість її застосування для багатьох практичних застосунків за умови виділення в мовному сигналі окремих структурних одиниць – фонем, чого досить складно досягнути з використанням інших моделей. Недоліками математичної вейвлет-моделі мовної інформації є складна процедура вибору міжфонемних меж у мовному сигналі. Суть процедури полягає в пошуку моментів збільшення вейвлет-коефіцієнтів на значній кількості рівнів масштабування. Також складноформалізованою процедурою є вибір базисних вейвлетів, основним призначенням яких є опис стаціонарних ділянок мовного сигналу за мінімальної кількості ненульових коефіцієнтів. За великої кількості квазістаціонарних та стаціонарних ділянок мовного сигналу кількість міжфонемних переходів збільшується, що, як наслідок, призводить до збільшення кількості шуканих вейвлетних базисів.

*Математичні моделі мовної інформації на основі імпульсно-модульованих сигналів.* Основним припущенням, яке приймається в ході побудови математичних моделей даної групи, є те, що мовна інформація містить вокалізовані мовні ділянки [40], які у формалізованому вигляді описуються функціональною залежністю параметрів моделі від часу з подальшим виділенням модулюючої (інформаційної) та модульованої (несучої) компоненти [26]. Зважаючи на значний різновид типів модуляції мовних сигналів [41]: амплітудної (відповідає за передавання фонетичної (звуковий склад) і просодичної (стать, вік, індивідуальні особливості мовника: інтонація, тембр, дикція, пауза, наголос, ритм тощо) складових мовної інформації) та частотної (відповідає за емоційний стан (висоту голосу) мовника), а також їх комбінацій. Як приклад, розглянемо імпульсний амплітудно-модульований сигнал. Найпростішу математичну модель імпульсного амплітудно-модульованого сигналу $u_{AM}(t)$ з декількома несучими частотами для випадку модуляції сумою гармонік та малості постійної складової несучого коливання через ослаблення гарнітурною або телефонною трубкою опишемо таким виразом [42]:

$$u_{AM}(t)=\sum_{k=0}^{K} M_k\cos\left(\Omega_k t+\Phi_k\right)\times \times\sum_{l=0}^{L} U_l\cos\left(\omega_l t+\varphi_l\right), t\in\left[0,\tau_{u_{AM}}\right], \quad (2)$$

де $M_k$ – глибина модуляції (відносна амплітуда) $k$ - ї гармоніки модулюючого коливання; $\Omega_k, \Phi_k$ – частота і фаза модулюючого коливання відповідно $k$ - ї гармоніки, $k=\overline{0,K}$; $U_l, \omega_l, \varphi_l$ – амплітуда, частота і фаза основного тону відповідно, $l=\overline{0,L}$; $\tau_{u_{AM}}$ – тривалість амплітудно-модульованого імпульсу.

Перевагою математичної моделі (2) є її висока точність, якої досягаємо в разі опису вокалізованих ділянок мовної інформації. Разом з тим досліджувана модель через накладені обмеження є ідеалізованою. Її застосування на практиці потребує урахування окрім вокалізованих та невокалізованих ділянок мовної інформації ще й усіх згаданих вище компонент її фонетичної та просодичної складових.

*Математичні моделі мовної інформації на основі хвильових рівнянь.* Хвильові математичні моделі ґрунтуються на основних положеннях акустичної теорії мовотворення, викладеної в [43]. У [18] показано, що в звуковому діапазоні на частотах до 4500 Гц акустичний тиск у мовному тракті можна описати одномірним хвильовим рівнянням, яке є модифікованим рівнянням Вебстера:

$$\frac{\partial^2 P}{\partial t^2}=c_0^2\frac{1}{S(x)}\frac{\partial}{\partial x}\left(S(x)\frac{\partial P}{\partial x}\right)-2\nu\frac{\partial P}{\partial t}+F(x,t),$$
$$0<x<l,\ t>0;$$
$$\left.\frac{\partial P}{\partial x}\right|_{x=0}=-\dot{q}(t),\ \left.\left(\frac{\partial P}{\partial x}-bP\right)\right|_{x=l}=0; \quad (3)$$
$$P(x,0)=P_0(x),\ \frac{\partial P}{\partial t}(x,0)=P_1(x),$$

де $\nu$ – джерело мовної інформації, $\nu=\frac{r_1}{2\rho}$; $q(t)$ – початкові профілі тиску та швидкості його зміни в тракті; $x$ – просторова координата вздовж середньої лінії тракту в середньосагітальній площині; $t$ – часовий момент; $P(x,t)$ – шуканий тиск у тракті; $S(x)$ – профіль площин поперечного перетину вздовж тракту; $F(x,t)$ – щільність розподілу джерел збурення всередині тракту; $c$ – швидкість звуку в тракті. Перевагою математичних моделей такого типу є можливість їх застосування для опису фрикативних звуків. Джерелом збурення фрикативних звуків, як відомо з [43], є шум турбулентного потоку повітря. До недоліків математичних моделей, що ґрунтуються на хвильових рівняннях, є обмеженість їх застосування, зумовлена достатньо невеликим частотним діапазоном, за межами якого вони втрачають свою адекватність. Крім того, моделі типу (3) не мають точного аналітичного рішення, а числові розв'язки, які отримуються внаслідок апроксимації джерел мовної інформації та пло-

щин поперечного перетину вздовж тракту, мають складну просторово-часову залежність, що призводить до неможливості їх практичного застосування для аналізу мовної інформації.

*Математичні моделі мовної інформації на основі методу лінійного передбачення* (моделі лінійного передбачення) є одними з найбільш адекватних математичних моделей аналізу мовних сигналів. Основна ідея їх розроблення полягає в лінійній апроксимації мовного сигналу лінійною комбінацією його попередніх відділків [44] на основі коефіцієнтів передбачення, під якими прийнято розуміти вагові коефіцієнти, що використовуються в лінійній комбінації.

У загальному вигляді математична модель мовної інформації на основі методу лінійного передбачення подається у вигляді моделі авторегресії [45], для якої поточний відлік $x[t]$ стаціонарного випадкового процесу з нульовим середнім визначається через попередні відліки $x[t-i]$ з деякими ваговими коефіцієнтами $\Phi[i]$, тобто

$$x[t]=\sum_{i=1}^{P}\Phi[i]x[t-i]+a[t], \qquad (4)$$

де $P$ – порядок моделі; $a[t]$ – некорельовані випадкові відліки.

Алгоритми знаходження коефіцієнтів авторегресійної моделі, а також дисперсії похибки передбачення визначають на основі повної системи лінійних рівнянь Юла-Уокера, яку ґрунтовно розкрито в [19], [44] та [45].

Основними перевагами моделей даного типу є охоплення ними широкого кола параметрів, які можуть бути враховані під час їх практичного застосування. Наприклад, такими параметрами є: функція площі мовного тракту, період основного тону, форманти, спектр, висока точність моделі та її відносна математична простота. Також серед переваг вирізняють можливість подання математичних моделей у вигляді мовних сигналів зі змінними в часі параметрами, збуджуваними квазіперіодичними імпульсами для вокалізованих ділянок та випадкових шумів для невокалізованих ділянок сигналу. Незважаючи на значну кількість переваг, порівняно з іншими динамічними моделями поданими у таблиці, математичні моделі мовної інформації на основі методу лінійного передбачення мають і недоліки. Основними з них є малий час передбачення моделі, а також потреба залучення додаткового джерела білого шуму для отримання визначених відліків сигналу математичної моделі. Внесення в конструкцію комплексу засобів захисту інформації додаткових джерел підвищує їх вартість та знижує конкурентну привабливість на ринку безпекових послуг в галузі ІТ.

*Гармонічні математичні моделі мовної інформації* – це найрозповсюдженіші типи моделей. Для задач криптографічного захисту інформації із зазначеного типу моделей найбільш прийнятною є дискретна модель $s(n)$, яка являє собою суму двох дискретних складових – періодичної $h(n)$ та шумової $r(n)$, тобто [46]:

$$s(n)=h(n)+r(n). \qquad (5)$$

У моделі (5) періодична складова визначається як $h(n)=\sum_{k=1}^{K}A_k(n)\cos\varphi_k(n)$, де $A_k(n)$ – миттєва амплітуда $k$-ї гармоніки $n$-ї дискрети мовної інформації; $K$ – кількість гармонік у сигналі; $\varphi_k(n)$ – миттєва фаза $k$-ї гармоніки $n$-ї дискрети мовної інформації ($\varphi_k(n)=\sum_{i=0}^{n}\frac{2\pi f_k(i)}{F_S}+\varphi_k(0)$, де $f_k(i)$ – миттєва частота $k$-ї гармоніки $i$-го відліку $n$-ї дискрети мовної інформації, $F_S$ – частота дискретизації, $\varphi_k(0)$ – початкова фаза $k$-ї гармоніки).

У ході практичного застосування моделі (5) частоти гармонік у кожен момент часу приймаються кратними частоті основного тону, тобто $f_k=k\,f_0$, де $k$ – номер гармоніки, а $f_0$ – частота основного тону. Однією з головних переваг моделі (5) є високий ступінь її адекватності, що досягається унаслідок декомпозиції гармонічного сигналу на періодичну (вокалізовану) і невокалізовану (шумову) складові. Аналіз досліджуваної моделі показує, що її точність залежить від кількості враховуваних гармонік та дискрет мовної інформації. Чим їх більше – тим модель точніша, чим точніша модель – тим вона складніша та, відповідно, неприйнятна в практичних застосунках, що є недоліком. Другий недолік випливає з першого. Точність моделі (5), окрім гармонік та дискрет, також обмежується нескінченною тривалістю гармонічної функції.

*Математичні моделі мовної інформації на основі інтегральних рівнянь Фредгольма першого роду (фредгольмові моделі)*

Вперше ідею застосування інтегральних рівнянь Фредгольма першого роду для опису моделей мовної інформації запропоновано в [18]. Для моделей такого типу вокалізована та невокалізована ділянки мовної інформації подаються у вигляді згортки функції збудження $z(s)$ і відгуку лінійного фільтра $K(x,s)$, який моделює мовний тракт [47]:

$$u(x)=\int_{0}^{x}K(x,s)\,z(s)\,ds. \qquad (6)$$

У термінах кібербезпеки [30] в моделі (6) прийнято такі позначення: $u(x)$ – шифрограма; $z(s)$ – мовна інформація, яка підлягає шифруванню; $K(x,s)$ – секретний ключ шифрування/розшифрування; $z(x)$ – розшифрована мовна інформація. З урахуванням зазначеного основною перевагою подання математичних моделей мовної інформації інтегральними рівняннями Фредгольма першого роду є гарантована криптостійкість шифрограм до відомих типів криптографічних атак [30].

Таблиця 1

Зведена таблиця за результатами аналізу переваг та недоліків математичних моделей мовної інформації

| Назва математичної моделі | Автор(и) математичної моделі | Математичний апарат | Формалізоване подання математичної моделі | | Ступінь відповідності досяжності мети | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | переваги | недоліки | *Дуже* | *Високий* | *Середній* | *Нижче се-* | *Низький* |
| **І КЛАС – динамічні моделі** | | | | | | | | | |
| **1** | **2** | **3** | **4** | | **5** | | | | |
| | | | **4.1** | **4.2** | **5.1** | **5.2** | **5.3** | **5.4** | **5.5** |
| **Вейвлет-модель** | Фарук М. Вишнякова О. Горшков Ю. та ін. | Вейвлет-перетворення | $s(t)=\sum_{k=0}^{N/2^n-1} s_{nk}\varphi_{nk}+\sum_{j=1}^{N}\sum_{k=0}^{N/2^n-1} d_{jk}\psi_{jk}$ | | | | | | |
| | | | • застосовується для розв'язання широкого кола практичних задач | • складна процедура вибору міжфонемних меж у мовному сигналі | | | | | |
| **Імпульсно-модульована модель** | Утробін В. Голубинський А. Лобанов Б. та ін. | Теорія електрозв'язку | $u_{AM}(t)=\sum_{k=0}^{K} M_k\cos(\Omega_k t+\Phi_k)\sum_{l=0}^{L} U_l\cos(\omega_l t+\varphi_l)$ | | | | | | |
| | | | • висока точність моделі | • високий ступінь ідеалізації моделі | | | | | |
| **Хвильова модель** | Фант Г. та ін. | Акустична теорія мовотворення | $\frac{\partial^2 P}{\partial t^2}=c_0^2\frac{1}{S(x)}\frac{\partial}{\partial x}\left(S(x)\frac{\partial P}{\partial x}\right)-2\nu\frac{\partial P}{\partial t}+F(x,t)$ | | | | | | |
| | | | • можливе застосування для опису фрикативних звуків, джерелом збурення яких слугує шум турбулентного потоку повітря | • невеликий частотний діапазон,у якому забезпечується адекватність моделі<br>• не мають точного аналітичного розв'язку | | | | | |
| **Моделі лінійного передбачення** | Рабинер Л. Тихонов А. Безрук В. та ін. | Теорія цифрового оброблення мовних сигналів | $x[t]=\sum_{i=1}^{P}\Phi[i]x[t-i]+a[t]$ | | | | | | |
| | | | • враховують значну кількість параметрів мовної інформації (функцію площі мовного тракту, період основного тону, форманти, спектр тощо)<br>• висока точність та відносна математична простота моделі<br>• подання математичних моделей у вигляді мовних сигналів зі змінними в часі параметрами, збуджуваними квазіперіодичними імпульсами для вокалізованих ділянок та випадковими шумами для невокалізованих ділянок сигналу | • малий час передбачення моделі<br>• потреба залучення додаткового джерела білого шуму для отримання визначених відліків сигналу<br>• підвищена вартість технічної реалізації засобів ТЗІ | | | | | |
| **Гармонічні математичні моделі** | Азаров І. Петровський та ін. | | $s(n)=h(n)+r(n)$ | | | | | | |
| | | | • моделі апробовані в прикладних задачах криптографічного захисту мовної інформації | • точність моделі залежить від кількості врахованих гармонік та | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | • високий ступінь адекватності, що досягається в наслідок декомпозиції гармонічного сигналу на періодичну (вокалізовану) і невокалізовану (шумову) складові | дискрет мовної інформації<br>• точність моделі обмежується нескінченною тривалістю гармонічних функцій | | | | | |
| **Фредгольмові моделі** | Сорокин В.<br>Келускар П.<br>Громико І.<br>та ін. | | $u(x)=\int_0^x K(x,s)\,z(s)\,ds$ | | | | | | |
| | | | • практичне застосування моделей забезпечує гарантовану криптостійкість мовної інформації;<br>• описують вокалізовані та невокалізовані складові мовної інформації | • моделі належать до класу обернених некоректних задач | | | | | |
| **II КЛАС – стохастичні моделі** | | | | | | | | | |
| **Акустико-фонетичні моделі** | Грачов А.<br>Огнев І.<br>Пилипенко В.<br>та ін. | **Приховані марковські процеси** | $\lambda=(A,B,\pi)$ | | | | | | |
| | | | • виступають підґрунтям для створення статистичних моделей фонем, слів та фраз<br>• висока точність моделей | • потреба у використанні великих, фонетично збалансованих, мовних баз даних<br>• залежність параметрів моделей тільки від їх попередніх станів | | | | | |
| **Моделі мовного трафіка** | Сахаров А.<br>Джаммул С.<br>та ін. | **Приховані марковські процеси** | Гамма-розподіл / Розподіл Вейбулла / Логонормальний розподіл /<br>/ Розподіл Пірсона / Бета-розподіл | | | | | | |
| | | | • описують на їх основі вокалізовані та невокалізовані складові мовної інформації для аналогових та цифрових систем зв'язку й передачі даних | • застосування моделі передбачає низку обмежень, зокрема, виконання умови постійної інтенсивності пакетів мовної інформації<br>• описують мовну інформацію у вигляді монологів | | | | | |

Другою вагомою перевагою є їх висока адекватність [18], [27], оскільки рівняння типу (6) містять усі необхідні й достатні параметри мовної інформації як вокалізованих, так і невокалізованих складових мовного сигналу. Наприклад, мовна інформація, яка підлягає шифруванню, може описуватися вокалізованими компонентами моделей (2) або (5).

Головним недоліком математичних моделей даного типу є їх належність до класу обернених некоректних задач за Адамаром, що виключає можливість точного відновлення мовної інформації без застосування методів регуляризації та додаткової апріорної інформації [29]. У контексті кіберзахисту мовної інформації даний недолік повинен розцінюватися як перевага, оскільки застосування математичних моделей, що ґрунтуються на інтегральних рівняннях Фредгольма першого роду, відкриває принципово нові можливості зі створення новітніх засобів криптографічного захисту.

*Результати аналізу математичних моделей мовної інформації 2-го класу*

Приховані марковські моделі мовної інформації є стохастичними моделями, в основу яких покладено марковські процеси. У науковій фаховій літературі їх інколи називають акустико-фонетичними моделями [32].

Найпростіша марковська модель мовної інформації $\lambda$ визначається як [34] :

$$\lambda=(A,B,\pi), \qquad (7)$$

де $A$ – матриця імовірностей переходів, $A=\{a_{ij}\}$, $a_{ij}$ – імовірність переходу системи зі стану $a_i$ у стан $a_j$; $B$ – матриця ймовірностей спостережень вихідних значень, $B=\{b_i(o_k)\}$, де $b_i(o_k)$ – імовірність того, що символ $0_k$ буде спостерігатися в системі, яка знаходиться в $a_i$ - му стані; $\pi=\{\pi_i\}$ – розподіл імовірностей початкового стану; $\pi_i$ – імовірність того, що $a_i$ є початковим станом системи. Приховані марковські моделі (6) є математичним базисом для створення низки статистичних моделей мовної інформації, а

саме: фонем, слів та фраз [34]. Наприклад, як показано в [48], статистична модель фонем для української мови на основі прихованих марковських моделей складається з трьох станів марковського ланцюга без пропусків, що дозволяє достатньо повно описувати 56 наявних фонем, включно з фонемою-паузою. У [49] та [50] показано, що основними перевагами моделей даного типу є їх висока точність та достатньо швидкий спосіб розрахунку значень функції відстані, а недоліком – потреба у використанні великих фонетично збалансованих мовних баз даних та залежність параметрів моделей тільки від їх попередніх станів.

Другим найбільш поширеним типом статистичних моделей є *математичні моделі мовних сигналів на основі "on / off"* послідовностей [35]. Їх математичний базис м становлять статистичні розподіли, зокрема: гамма; Вейбулла, логонормальне; Пірсона; бета-розподіл. Один зі способів розроблення математичної моделі мовної інформації розкрито в [35]. Його суть полягає в побудові моделі за рахунок підбору функцій щільності розподілу ймовірностей появи інтервалів з мовою та паузами визначеної тривалості. Модель мовної інформації, яку в [35] названо моделлю мовного трафіка, складається з *on*-та *off*-інтервалів, що чергуються. Значення *on*-інтервалів відповідає тривалості інтервалів мовлення, а *off*-інтервали описують паузи, під час яких мовна інформація не передається.

Перевагою даного типу моделей є можливість опису на їх основі вокалізованих та невокалізованих складових мовної інформації для аналогових і цифрових систем зв'язку й передачі даних. Математичні моделі мовних сигналів на основі *"on / off"* послідовностей дозволяють моделювати лише монологи, що є їх суттєвим недоліком. Також проблемним питанням, яке ускладнює практичне застосування цих моделей, є вибір функцій розподілу випадкових величин, які описують *on-* та *off*-інтервали, що для аналогових та цифрових детекторів є різними [36].

**Висновки.** На основі проведеного аналізу математичних моделей мовної інформації, їх переваг та недоліків у статті закладено теоретичне підгрунтя для вибору такої математичної моделі, яка дозволяє враховувати індивідуальні особливості джерела мовної інформації та має прийнятну реалізованість для заданої системи параметрів моделі. У результаті дослідження розроблено підхід до створення новітніх засобів криптографічного захисту мовної інформації в IP-мережах, які грунтуються на нових, некласичних типах математичних моделей.

**ЛІТЕРАТУРА**

[1] Левченко О. В. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування: монографія / О. В. Левченко – Житомир: ЖВІ, 2020. – 180 с.

[2] Грищук Р. В. Основи кібернетичної безпеки: Монографія / Р. В. Грищук, Ю. Г. Даник; за заг. ред. проф. Ю. Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.

[3] Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. Відомості Верховної Ради України. 2017, № 45, 403 с.

[4] Розум І. Ю. Шляхи і напрями розвитку системи зв'язку та автоматизації управління в інтересах військового управління / І. Ю. Розум // Збірник наукових праць Національної академії Державної прикордонної служби України. – №1. – 2014. – С. 162–174.

[5] Kumar, V. & Roy, O.P., (2021). Reliability and security analysis of VoIP communication systems. In Rising Threats in Expert Applications and Solutions (pp. 687-693). Springer, Singapore.

[6] Mentsiev A. VoIP security threats [Електронний ресурс] / A. Mentsiev, A. Dzhangarov // Инженерный вестник Дона. – 2019. – Режим доступу до ресурсу: http://surl.li/bbjxs.

[7] Kaur J. The recent trends in cyber security: A review / J. Kaur, R. Ramkumar // Journal of King Saud University –Computer and Information Sciences. – 2021. – pp. 1–16.

[8] Lauder A. Limits of Control: Examining the Employment of Proxies by the Russian Federation in Political Warfare Matthew / A. Lauder // Journal of Future Conflict. - Issue 01. – 2019. – pp. 1–46.

[9] Парамонов П. А. Методы, алгоритмы и устройства рапсознавания речи в ассоциативной осцилляторной среде : дис. канд. техн. наук : 05.13.05 / Парамонов П. А. – Москва, 2015. – 147 с.

[10] Борисов А. В. Моделирование и мониторинг состояния VoIP-соединения / А. В. Борисов, А. В. Босов, Г. Б. Миллер // Информатика и ее применения. – 2016. – Т. 10. – № 2. – С. 2–13.

[11] Дудикевич В. Б. Інформаційна модель безпеки технологій зв'язку / В. Б. Дудикевич, В .О. Хорошко, Г. В. Микитин та ін. // Інформатика та математичні методи в моделюванні. – Т. 4, № 2 – 2014. – С. 137–148.

[12] Грищук О. М. Симетрична криптосистема на диференціальних перетвореннях як новий засіб забезпечення кібербезпеки VoIP-трафіку / О. М. Грищук // Стратегії кіберстійкості: управління ризиками та безперервність бізнесу: Матеріали Всеукраїнської науково-практичної Інтернет конференції (м. Київ, 25 лютого 2021 року). Навчально-науковий інститут захисту інформації, Державний університет телекомунікацій. Київ, 2021. – С. 51–52.

[13] Гончарова С. В. Алгоритм додаткового криптографічного захисту голосових даних / С. В. Гончарова, Д.І. Могилевич // Наукова конференція «Проблеми телекомунікацій 2016», 19 - 22 квітня. – Київ, 2016. – С. 405–408.

[14] Смирнов В. В. Разработка системы защиты корпоративных цифровых линий связи / В. В. Смирнов, Н. Ю. Паротькин // Новейшие достижения и успехи развития технических наук – 2016. – С. 48–51.

[15] СКАТ-Е: шифратор з інтегрованим модулем перетворення мовної інформації [Електронний ресурс] // Трител. – 2016. – Режим доступу до ресурсу: https://cutt.ly/CUKepeA.

[16] Голубинский А. Н. Модели речевых сигналов для аутентификации личности по голосу : дис. докт. техн. наук : 05.13.18; 05.13 / Голубинский А. Н. – Воронеж, 2010. – 403 с.

[17] Лобанов Б. М. Речевой интерфейс интеллектуальных систем / Б.М. Лобанов, О.Е. Елисеева; под науч. ред. В.В. Голенков. – Минск: БГУИР, 2006. –152 с.

[18] Сорокин В. Н. Фундаментальные исследования речи и прикладные задачи речевых технологий / В. Н. Сорокин // Речевые технологии. – 2008. – № 1. – С. 18–48.

[19] Рабинер Л. Р. Цифровая обработка речевых сигналов / Л. Р. Рабинер, Р. В. Шафер. Под ред. М. В. Назарова и Ю. Н. Прохорова. – М. : Радио и связь, 1981. – 496 с.

[20] Гапочкин А. В. Классификация речевых сигналов / А. В. Гаппочкин // Вестник МГУП имени Ивана Федорова. – 2015. – № 1. – С. 43–50.

[21] Алимурадов А. К. Обзор и классификация методов обработки речевых сигналов в системах распознавания речи / А. К. Алимурадов, П. П. Чураков // Измерение. Мониторинг. Управление. Контроль. – 2015. – № 2 (12). – С. 27–35.

[22] Singh N. Digital Signal Processing for Speech Signals / N. Singh, R. A. Khan // Bilingual International Conference on Information Technology: Yesterday, Toady, and Tomorrow, 19-21 Feburary 2015. – 2015. – С. 134–138.

[23] Kumar T. S. Classification of voiced and non-voiced speech signals using empirical wavelet transform and multi-level local patterns / T. S. Kumar, M. A. Hussain, V. Kanhangad // International Conference on Digital Signal Processing, DSP, 2015. – Vol. 2015-September. – pp. 163–167.

[24] Stylianou Y. Apply the harmonic plus noise model in concatenative speech synthesis / Y. Stylianou // IEEE Trans. on Speech and Audio Process. – 2001. – Vol. 9. – № 1. – pp. 21–29.

[25] Kafentzis G. Adaptive Sinusoidal Models for Speech with Applications in Speech Modifications and Audio Analysis: дис. докт. Філос.: Signal and Image processing / G. Kafentzis – Université Rennes; Panepistīmio Krītīs. – 2014. – 200 p.

[26] Голубинский А. Н. Математическая модель речевого сигнала, основанная на аппроксимации спектра набором постоянных составляющих в соответствующих полосах частот / А.Н. Голубинский // Безопасность информационных технологий. – 2009. - № 2. – С. 12–18.

[27] Криптография нового поколения: Интегральные уравнения как альтернатива алгебраической методологии / Г.К. Броншпак, И.А. Громыко, С.И. Доценко, Е.Л. Перчик // Прикладная электроника. – 2014. – Т. 13, №3. – С. 337-349.

[28] Леонов А. С. О точности определения параметров голосового источника / А. С. Леонов, В. Н. Сорокин // Акустический журнал. – Т. 60, № 6. – 2014. – С. 656–662.

[29] Речевые обратные задачи и ресинтез [Електронний ресурс] / А. С.Леонов, И. С. Макаров, В. Н. Сорокин, А. И. Цыплихин // Акустический институт им. акад. Н. Н. Андреева. – 2019. – Режим доступу до ресурсу: http://surl.li/bcido.

[30] Грищук Р. В. Узагальнена модель криптосистеми Фредгольма / Р. В. Грищук, О. М. Грищук // Кібербезпека: освіта, наука, техніка. – 2019. – № 4. – С. 14–23.

[31] Применение современных технологий распознавания речи при создании лингвистического тренажера для повышения уровня языковой компетенции в сфере межкультурной коммуникации / Д. С. Колесникова, А. К. Рудниченко, Е. А. Верещагина и др. // Интернет-журнал "Науковедение". – Т. 9 (№ 6). – 2017. – С. 1–12.

[32] Грачев А. М. Статистические подходы к автоматическому распознаванию речи / А. М. Грачев // Вестник Нижегородского университета им. Н.И. Лобачевского, 2015 – № 2 (2). – С. 376–379.

[33] Bryan J. D. Autoregressive Hidden Markov Model and the Speech Signal / J. D. Bryan, S. E. Levinson // Procedia Computer Science. – 2015. – №61. – С. 328–333.

[34] Огнев И. В. Распознавание речи методами скрытых марковских моделей в ассоциативной осцилляторной среде / И. В. Огнев, П. А. Парамонов. // Технические науки. Информатика, вычислительная техника. – 2013. – С. 115–126.

[35] Сахаров А. В. Статистические модели трафика ip-телефонии : автореф. дис. на соиск наук. степени канд. техн. наук : спец. 05.13.01 "Системный анализ, управление и обработка информации" / Сахаров А. В. – Нижний Новгород, 2007. – 16 с.

[36] Джаммул С. Х. Идентификация трафика сетей передачи данных в реальном времени : дис. канд. техн. наук : 05.13.17 – Теоретические основы информатики / Джаммул С. Х. – М, 2018. – 143 с.

[37] Farouk, M. H. Application of wavelets in speech processing [Text] : monogr. / M. H. Farouk. – Springer, 2014. – 53 p.

[38] Вишнякова О. А. Автоматическая сегментация речевого сигнала на базе дискретного вейвлет-преобразования / О. А. Вишнякова, Д. Н. Лавров // Математические структуры и моделирование. – Вып. 11. – 2011. – С. 43–48.

[39] Горшков Ю. Г. Обработка речевых сигналов на основе вейвлетов / Ю. Г. Горшков // T-Comm: Телекоммуникации и транспорт. – 2015. – №2. – С. 46–53.

[40] Утробин В. А. Алгоритм выделения вокализованных участков речевого сигнала / В. А. Утробин, В.Е. Гай // Вестник Нижегородского университета им. Н.И. Лобачевского, 2012. – № 6 (1). – С. 175–179.

[41] Лобанов Б. М. Компьютерный синтез и клонирование речи : моногрфия / Б. М. Лобанов, Л. И. Цирульник. – Минск : Белорусская наука, 2008. – 316 с.

[42] Голубинский А.Н. Выделение модулирующего колебания из огибающей речевого сигнала / А.Н. Голубинский, О.М. Булгаков // Системы управления и информационные технологии. – 2009. – № 4.1. – С. 130–134.

[43] Фант Г. Акустическая теория речеобразования: моногр. / Г. Фант. // Г. Фант Перевод с англ. Л. А. Варшавского и В.И. Медведева. Под ред. В. С. Григорьева. – М. : Наука, 1964. – 284 с.

[44] Рабинер Л. Р. Цифровая обработка. Маркел Дж. Д. Линейное предсказание речи : перев. с англ. / Дж. Д. Маркел, А. Х. Грэй. Под. ред. Ю. Н. Прохорова и В. С. Звездина. – М. : Связь, 1980. – 308 с.

[45] Распознавание дикторов по частотам параметрических спектров в модели речи в виде составных векторных случайных процессов / В.А. Тихонов, В.М. Безрук, Н.В. Хмеларжова (Кудрявцева), П. Хмеларж // Наукомісткі технології в інфокомунікаціях: обробка, захист та передача інформації: Монографія

/ під загальною редакцією В. М. Безрука, В. В. Баранніка. – ФОП Бровін О.В., Харків. – 2018. – С. 199–220.

[46] Азаров И. С. Вычисление мгновенных гармонических параметров речевого сигнала / И. С. Азаров, А. А. Петровский // Речевые технологии. – № 1. – 2008. – С. 67–77.

[47] Келускар П. Н. Система управления распознаванием речевой информации: бакал. раб: техника и технологии / Келускар П. Н. – Таганрог, 2008. – 91 с.

[48] Пилипенко В. В. Опыт автоматического стенографирования украинской парламентской речи / В. В. Пилипенко, В. В. Робейко // Речевые технологии. – № 3. – 2009. – С. 34–46.

[49] Балакшин П. В. Алгоритмические и программные средства распознавания речи на основе скрытых марковских моделей для телефонных служб поддержки клиентов : дис. канд. техн. наук : 05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей / Балакшин П. В. – Санкт-Петербург, 2014. – 127 с.

[50] Бабин Д. Н. О перспективах создания системы автоматического распознавания слитной устной русской речи / Д. Н. Бабин, И. Л. Мазуренко, А. Б. Холоденко // Интеллектуальные системы. – 2004. – Т. 8, 1-4. – С. 45–70.

**УДК 004.056**

***Korchenko O., Hryshchuk O. Comparative analysis of mathematical models of speech information***

***Abstract.*** *The aggravation of the cyber security situation around Ukraine requires a radical revision of the current approaches to ensuring the cyber security of information and telecommunication systems of the state. Anticipatory pace of development of means and technologies of cyberattack determines the need to find new non-trivial (asymmetric) and at the same time practical ideas aimed at ensuring cyber security of information regardless of the type of its presentation. Recently, speech information that circulates in IP networks has become the object of cyberattacks by unscrupulous competitors, foreign government institutions, and simply interested individuals. As known, one of the most effective measures of cyber security of speech information is its cryptographic protection. Well-known international and national cryptographic protocols provide sufficient cryptographic stability, but despite this, the number of cyber threats to speech information does not decrease, but, on the contrary, increases in proportion to the growth of its value. Therefore, the issue of increasing the level of security of speech information that circulates in IP networks remains relevant. One of the first stages on the way to the creation of the latest cryptographic means of protecting speech information is the analysis of relevant mathematical models. In order to establish the advantages and disadvantages of known mathematical models of speech information and choose among them with the same accuracy the one that will consider the individual features of the source of speech information, as well as have an acceptable realizability for a given system of parameters, the article presents the results of the analysis of two classes of models: dynamic and stochastic. It is shown that the main dynamic models of speech information, which belong to the models of the first class, are wavelet models, pulse-modulated and wave models, models of linear prediction, harmonic mathematical models. In the article, in addition to the well-known mathematical models of the first class, a new type of them is analyzed - Fredholm models of speech information. The second class of models considered in the article includes two of the most common types, namely: acoustic-phonetic models and speech traffic models. For each of the researched models of one or another class and type, developers were established, the mathematical apparatus underlying them was specified, and the researched mathematical model of speech information is formalized. On the basis of the introduced qualitative scale, based on the totality of the determined advantages and disadvantages of the analyzed models, the degree of achievement of the obtained results was assessed in accordance with the goal set in the article. Therefore, the conducted analysis covered the most common classes of mathematical models of speech information and made it possible to choose among them the one that will become the basis for the development of the latest cryptographic means of protection.*

***Key words:*** *mathematical model, speech information, comparative analysis, cyber security, IP network, VoIP telephony, cryptographic attack, cryptographic protection*

**Корченко Олександр Григорович,** д.т.н., професор, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету.

**Oleksandr Korchenko,** doctor of technical sciences, professor, head of the department of security of information technologies of the National Aviation University.

**Грищук Ольга Михайлівна,** науковий співробітник науково-дослідного відділу інформаційної та кібернетичної безпеки Житомирського військового інституту імені С. П. Корольова.

**Olga Hryshchuk,** researcher of the information and cyber security research department of the Zhytomyr Military Institute named after S.P. Korolev.

Отримано *3 червня 2022 року,* затверджено редколегією *14 листопада 2022 року*