УДК 004.056 **DOI:10.30837/rt.2022.1.208.01**

І.Д. ГОРБЕНКО, д-р техн. наук, О.А. ЗАМУЛА, д-р техн. наук

НАУКОВИЙ ПІДХІД ДО ЙМОВІРНІСНОЇ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ ВІД НАВ'ЯЗУВАННЯ ХИБНИХ ПОВІДОМЛЕНЬ У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Вступ

Функціонування цілої низки сучасних телекомунікаційних систем (ТКС), здійснюється в умовах зовнішніх і внутрішніх впливів, обумовлених, з одного боку, дією природних перешкод, перешкод від інших радіотехнічних систем, що функціонують на близьких частотах або в спільній ділянці діапазону частот, з іншого боку,- навмисних впливів, у тому числі, кібератак, створюваних зловмисником з метою руйнування, радіоелектронного подавлення діючих систем [1-2]. Об'єктивно існують загрози кібер - і інформаційної безпеки, а саме можливість: несанкціонованого доступу до інформаційних активів, порушення цілісності, конфіденційності, доступності даних, фальсифікація повідомлень з боку зловмисників тощо. Вищезазначене може призвести до суттєвого погіршення показників функціонування ТКС. Тому, до ТКС, особливо, таких, що функціонують на об’єктах критичної інфраструктури, пред'являються все більш жорсткі вимоги щодо забезпечення ефективності їх функціонування: достовірності і швидкості передачі інформації, живучості, завадозахищеності, кібер- і інформаційної безпеки. У таких умовах особливого значення набуває наявність і застосування захищених ТКС. У істотній мірі такі системи повинні базуватися на застосуванні захищених радіоканалів. Під захищеністю систем необхідно розуміти, в широкому сенсі, перш за все, їх здатність забезпечувати необхідні показники з завадозахищеності, імітостійкості, інформаційної, енергетичної і структурної скритності, швидкості передавання інформації, частотної і енергетичної ефективності. Завдання побудови захищеної ТКС – створити систему, стійку до впливу безлічі різноманітних, актуальних для даної системи, впливів, у тому числі кібератак. При цьому, об'єктивно існує суперечність між жорсткими вимогами щодо забезпечення достовірності, скритності, конфіденційності, цілісності, справжності даних, що зберігаються та передаються по провідних та бездротових лініях зв'язку ТКС, з одного боку, і існуючими моделями, методами та технологіями управління телекомунікаційними мережами, інформаційною безпекою, якістю обслуговування, з іншого боку [3-4].

Основними шляхами вирішення даної суперечності є підвищення завадозахищеності та кібер і інформаційної безпеки ТКС на основі удосконалення методологічних основ побудови ТКС шляхом отримання нових наукових підходів до оцінки реального стану захищеності ТКС, і створення моделей, методів та технологій захисту від існуючих кіберзагроз і загроз інформаційної безпеки.

Основні результати досліджень

Широке застосування хмарних обчислень, засобів віддаленого підключення з мобільних та віддалених стаціонарних пристроїв через мережі загального призначення призводять до «зникнення периметра» критичних систем та значного ускладнення забезпечення їхнього безпечного функціонування. Тому забезпечення безпеки телекомунікаційних систем стало одним із пріоритетних завдань у сучасному світі. В умовах внутрішніх та зовнішніх несанкціонованих дій порушників щодо ТКС фактично для будь-якого повідомлення, блоку даних або програмного коду необхідно реалізувати ряд послуг (функцій) безпеки.

До основних функцій (послуг) інформаційної безпеки слід віднести такі [5].

Конфіденційність інформації - властивість захищеності інформації (із наперед заданою якістю (ймовірністю)) від несанкціонованого доступу до неї та спроб розкриття (отримання змісту) неавторизованими користувачами та (або) процесами.

Цілісність інформації - властивість захищеності інформації, яке полягає в тому, що інформація практично не може бути змінена випадково чи навмисно неавторизованими суб'єктами (порушниками) або об'єктами (процесами), причому факт можливості порушення цілісності може бути визначений наперед заданою ймовірністю.

Справжність (автентичність) - властивість об'єктів/суб'єктів (зокрема інформації, ресурсів, повідомлень, даних, користувачів тощо.) забезпечити встановлення достовірності твердження у тому, що суб'єкт чи об'єкт має заявлені (очікувані) властивості.

Доступність - властивість ресурсу системи (інформації, послуги, об'єкта інформаційної та (або) телекомунікаційної системи), яке полягає в тому, що авторизований користувач та (або) процес, наділений відповідними повноваженнями, може використовувати ресурс відповідно до правил та певної якості.

Невідмовність – властивість, пов'язана із запобіганням можливості заперечення реальними суб'єктами (користувачами) та об'єктами (процесами) фактів повного чи часткового брати участь в інформаційному обміні чи інформаційній взаємодії. Як правило, включає формування, надання та передачу доказів реального участі в інформаційному обміні або інформаційній взаємодії.

Спостереженість - властивість ресурсу системи (комп'ютерної системи, об'єкта комп'ютерної системи тощо), що дозволяє реєструвати (фіксувати) дії користувачів та процесів, використання ресурсу системи, однозначно встановлювати ідентифікатори (імена) причетних до певних подій користувачів та процесів, а також реагувати на ці події з метою мінімізації можливих втрат у системі здійснюється, у тому числі, за рахунок використання криптографічних перетворень.

Зазначені послуги повною мірою можуть бути реалізовані за допомогою використання симетричних та асиметричних криптографічних перетворень та протоколів.

До основних механізмів забезпечення справжності, цілісності, автентичності повідомлень відносять алгоритми шифрування даних, електронні цифрові підписи, коди автентифікації повідомлень (MAC коди) та ін.

MAC код [5] - це функція відображення h: $K \times D \to R$, где $K = \{0,1\}^n$ – простір ключів, $D = \{0,1\}^*$ – простір повідомлень, а $R = \{0,1\}^n$ – простір MAC значень для k, $n \geq 1$. Для заданих значень ключа $k \in K$ і повідомлення $X \in D$, функція виробляє MAC значення $Y \in R$.

Наведемо визначення та сформулюємо пропозиції щодо забезпечення стійкості кодів автентифікації повідомлень до різних атак з боку станції протидії. Покажемо можливість застосування наведених результатів задля забезпечення істинності та цілісності повідомлень.

Розглянемо випадок, коли зловмисник може підробити повідомлення для MAC коду, якщо, не знаючи випадкового ключа, він здатний створити нове повідомлення X та MAC значення Y таке, що $h(K, X) = Y$.

Введемо визначення: MAC код $h: K \times M \to R$ є $(t; \varepsilon; q)$ секретним, якщо, при випадково взятому ключі K, зловмисник не може підробити нове повідомлення за час t з ймовірністю вище за ε, навіть якщо він (на свій вибір) має можливість отримати q значень MAC кодів інших повідомлень.

Залежно від інформації, доступної зловмиснику, розрізняють такі типи атак на коди автентифікації повідомлень [5].

1. Атака із відомим текстом. Зловмисник має можливість досліджувати деякі відкриті тексти та відповідні значення коду автентифікації повідомлень.

2. Атака із вибраним текстом. Порушник має можливість вибирати набори текстів та згодом отримувати значення кодів автентифікації повідомлень, що відповідають вибраним текстам.

3. Атака із адаптивним вибором тексту. Це найбільш загальна атака, коли зловмисник вибирає текст і негайно набуває відповідних значень коду автентифікації повідомлення.

4. Угадування коду автентифікації повідомлення (Guessing of the MAC). Це пряма атака на алгоритм MAC коду і полягає у виборі будь-якого нового повідомлення і, згодом, вгадування значення коду автентифікації повідомлення. Вона може бути виконана такими способами:

– вгадування ключа, з наступним обчислення значення MAC коду, з ймовірністю успіху 2^{-n}, n-позначає розмір (у бітах) значення MAC коду.

– вгадування ключа, з наступним обчислення значення MAC коду, з ймовірністю успіху 2^{-k}, k - довжина (в бітах) секретного ключа.

Цей тип атаки не піддається перевірці і, отже, порушник апріорі не знає, чи він вгадав значення MAC коду. Успіх атаки (досягнення очікуваного результату) залежить від кількості спроб здійснення атак.

Вичерпний пошук ключа (Exhaustive Key Search). Атака вимагає приблизно k/n відомих пар тексту MAC для фіксованого ключа. Намагаючись визначити ключ, крипто аналітик перебирає один за одним усі можливі ключі. Очікуване число випробувань, яке призведе до злому алгоритму MAC, дорівнює k/n . На відміну від попередньої атаки, цю атаку можна здійснювати поза сеансом зв'язку (off-line).

Підробка, заснована на внутрішній колізії (Internal Collision Based Forgery). Наслідок цієї атаки полягає в тому, що якщо виявити внутрішню колізію (збіг проміжних результатів при обчисленні значень MAC кодів), її можна використовувати для підробки MAC коду окремо вибраного тексту.

Виконаємо оцінку стійкості MAC кодів при імітації та заміні.

Аналіз показує, що з метою заміни повідомлень, порушник повинен сформувати повідомлення x' та відповідний повідомленню автентифікатор $y' = f(x')$. Це може бути виконано двома способами: шляхом імітації та шляхом підміни.

У разі імітації порушник формує автентифікатор $y = f(x)$ є дійсним [6]:

$$\mathrm{P_{им}} = \mathrm{P}\left(\mathrm{y} = \mathrm{f}\left(\mathrm{x}\right) - \text{истинно}\right), \left(\mathrm{x}, \mathrm{y}\right) \in \mathrm{A} \times \mathrm{B},\ \mathrm{f} \in \mathrm{H} \tag{1}$$

При рівно ймовірному виборі ключа, що еквівалентно вибору $f \in H$, необхідно враховувати розподіл MAC значень y конкретного повідомлення по ключовому простору. Для ймовірності імітації, позначимо її як ймовірність імітації за ключем $\mathrm{P_{имКл}}$, справедливо наступне вираз:

$$\mathrm{P_{имКл}} = \frac{\left|\left\{\mathrm{f} \in \mathrm{H} : \mathrm{y} = \mathrm{f}\left(\mathrm{x}\right)\right\}\right|}{\left|\mathrm{H}\right|}, (\mathrm{x}, \mathrm{y}) \in \mathrm{A} \times \mathrm{B}, \tag{2}$$

де $\left|\left\{f \in H : y = f(x)\right\}\right|$ - кількість хеш-функцій f, які породжують повідомлення x значення MAC коду y.

Очевидно, що

$$\mathrm{P_{имКл}} \geq \frac{1}{\left|\mathrm{H}\right|}. \tag{3}$$

Крім того, всі записи в стовпцях масиву МАС кодів зустрічаються однакову кількість разів і тому маємо: $P_{\text{имКл}} \geq \frac{1}{|B|}$.

Тому верхня межа ймовірності імітації МАС коду по ключу визначається максимальним значенням $P_{\text{имКл}} \geq \frac{1}{|B|}$ по всьому просторі повідомлень, а значення ймовірності $P_{\text{им}Кл}$ визначається наступним співвідношенням:

$$P_{\text{имКл}_{x\in A}} \leq \max \frac{\left|\left\{f \in H : y = f(x)\right\}\right|}{|H|}, (x, y) \in A \times B. \quad (4)$$

Якщо не зважати на розподіл МАС значень y для даного повідомлення по ключовому простору, тоді ймовірність імітації позначимо як ймовірність імітації за МАС значенням $P_{\text{имМАС}}$. Імітація за допомогою нав'язування МАС значення визначається тим, що з множини передбачуваних МАС кодів вибирається одне. Імовірність успіху визначатиметься виразом:

$$P_{\text{имМАС}} = \frac{1}{\left|\left\{y \in B : y = f(x)\right\}\right|}, (x, y) \in A \times B. f \in H, \quad (5)$$

де $\left|\{y \in B : y = f(x)\}\right|$ - потужність безлічі можливих МАС значень для повідомлення x.

Якщо МАС значення для повідомлення x набувають повної кількості значень $|B|$, отримаємо

$$P_{\text{имМАС}} = \frac{1}{|B|}. \quad (6)$$

У загальному випадку справедлива така нижня межа:

$$P_{\text{имМАС}} \geq \frac{1}{|B|}. \quad (7)$$

Якщо для повідомлення відомий статистичний розподіл МАС значень, оцінка ймовірності імітації за МАС значенням зводиться до оцінки ймовірності імітації за ключем. Верхня межа для ймовірності імітації за МАС значенням визначатиметься максимальним значенням по всьому просторі повідомлень:

$$P_{\text{имМАС}} \leq \max \frac{1}{\left|\left\{y \in B : y = f(x)\right\}\right|}, y \in B. f \in H \cdot \quad (8)$$

Атака підміни полягає в тому, що порушник спостерігає (x, y) і змінює його на (x', y'), де $x \neq x'$. Імовірність заміни визначатиметься умовною ймовірністю:

$$P_{\text{под}} = P(f(x') = y' - \text{истинно} \,|\, f(x) = y), \quad (x,y), (x',y') \in A \times B, x \neq x', f \in H \quad (9)$$

Вираз для ймовірності заміни з використанням формули повної ймовірності та статистики спостережень виглядатиме як:

$$P_{\text{под}} = \frac{\left|\left\{f \in H : y = f(x), y' = f(x')\right\}\right|}{\left|\left\{f \in H : y = f(x)\right\}\right|}, (x, y), \left(x', y'\right) \in A \times B, x \neq x', f \in H. \quad (9)$$

Верхня межа ймовірності нав'язування шляхом підміни повідомлень та МАС визначається максимальною ймовірністю успіху для всіх пар повідомлень, але за умови рівно ймовірного вибору ключа.

Аналіз показує, що можливі два випадки, коли заміна повідомлення x на x', якщо $x \neq x'$ здійснюється з тим самим автентифікатором $y = y'$, (заміна першого роду) і з різними $y \neq y'$ (підміна другого роду).

Імовірність заміни за умови рівності $y = y'$ визначається ймовірністю колізії МАС коду та оцінюється виразом:

$$P_{под1} \leq P_{кол} = \max \frac{\left|\left\{f \in H : y = f(x), y' = f(x')\right\}\right|}{\left|\left\{f \in H : y = f(x)\right\}\right|}, (x,y),(x',y') \in A \times B, x \neq x', f \in H. \quad (10)$$

Для ймовірності заміни другого роду маємо:

$$P_{под2} \leq \max \frac{\left|\left\{f \in H : y = f(x), y' = f(x')\right\}\right|}{\left|\left\{f \in H : y = f(x)\right\}\right|}, (x,y),(x',y') \in A \times B, x \neq x', y \neq y', f \in H. \quad (11)$$

Таким чином, для точного обчислення імітаційної та колізійної стійкості МАС кодів за наведеними формулами необхідно використовувати статистику спільних розподілів МАС кодів за ключами для дійсних та підроблених повідомлень. Для МАС кодів визначення такої статистики видається проблематичним через дуже великий розмір масиву можливих МАС. Нижні межі для ймовірностей імітації та підміни не враховують статистичні властивості масивів автентифікаторів, і ґрунтуються на моделі псевдовипадковості функції f(x) та визначають мінімальні вимоги до розміру ключового простору та простору МАС значень.

Верхні межі для ймовірностей імітації та підміни пов'язані з комбінаторними властивостями МАС масивів та оцінюють значення колізій у просторі А х В для найгіршого випадку вибору ключів та повідомлень.

Розглянемо колізійні властивості МАС кодів.

Під стійкістю до колізій розуміють обчислювальну складність знаходження двох повідомлень M_i і M_j таких, що [1]:

$$H(M_i) = H(M_j), \quad (12)$$

де Н є відповідним перетворенням.

У [6] наводяться оцінки ймовірності створення колізій, причому вважається, що для реалізації колізії необхідно виконати не менше $\sqrt{n}$ експериментів із загальної кількості можливих значень n.

Математична постановка завдання ймовірнісної оцінки колізій формулюється в такий спосіб.

Нехай є деяка функція перетворення Н повідомлення М

$$h = H(M), \quad (13)$$

де М - це повідомлення довільної довжини l_M, причому h може набувати значення $n = 2^m$ незалежно від довжини l_M. Необхідно визначити число випадкових повідомлень k, які необхідно подати на вхід перетворювача Н, щоб з ймовірністю $P_з$ відбувся хоча б один збіг виду (12), тобто колізія.

Оцінка кількості випробувань появи колізій

Проведений аналіз показав, що при розв'язанні даної задачі має місце вибірка з значень цілісної випадкової величини з рівноймовірним законом розподілу, що приймає значення від 1 до $n = 2^m$, а $k \le n$.

У таких умовах необхідно знайти ймовірність $P(n,k)$ того, що з значень H(M) вибірки, по крайній мірі, дві збігаються, тобто: $H(M_i) = H(M_j)$.

Для вирішення сформульованої задачі знайдемо ймовірність того, що в групі з подій не відбудеться колізія, тобто співвідношення (12) не виконається жодного разу. Позначимо цю можливість як $R(n,k)$. Зрозуміло, що $P(n,k)$ і $R(n,k)$ становлять повну групу подій, тобто: $P(n,k)+R(n,k)=1$, і

$$P(n,k)=1-R(n,k). \tag{14}$$

Далі знайдемо загальну кількість N різних способів, якими можна отримати значень без повторень. Для першого елемента маємо n значень без повторень, для другого n - 1, для третього – n - 2 тощо, для k - го – (n-k+1). Тому загальна кількість способів, за яких немає збігів може бути розраховано як:

$$N = n\cdot(n-1)(n-2)\ldots(n-k+1) = \frac{n!}{(n-k)!}. \tag{15}$$

Оскільки при кожній з подій з однаковою ймовірністю може відбуватися кожна з подій, то загальну кількість подій можна оцінити як

$$N_{\sum} = n^k. \tag{16}$$

Імовірність відсутності збігів можна оцінити ставленням числа варіантів без збігів (15) до загального числа варіантів (16), тобто

$$R(n,k) = \frac{\frac{n!}{(n-k)!}}{n^k} = \frac{n!}{(n-k)!n^k}. \tag{17}$$

Тоді, вираз для визначення $P(n,k)$ буде мати вигляд:

$$P(n,k)=1-\frac{n!}{(n-k)!n^k}. \tag{18}$$

Бажано отримати загальне рішення рівняння (18), наприклад, для значення k. З цією метою представимо $P(n,k)$ у вигляді:

$$P(n,k)=1-\frac{n(n-1)\ldots(n-k+1)}{n^k}=1-\left[\frac{n-1}{n}\,\frac{n-2}{n}\ldots\frac{n-k+1}{n}\right]=$$

$$=1-\left[\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\ldots\left(1-\frac{k-1}{n}\right)\right]. \tag{19}$$

Далі скористаємося тим, що всіх $1 > x \ge 0$ [2] справедливим є:

$$(1-x) \le e^{-x}.$$

З огляду на це, отримаємо:

$$\mathrm{P}\left(\bar{\mathrm{n}},\mathrm{k}\right)=1-\left(\mathrm{e}^{-\frac{1}{\mathrm{n}}}\mathrm{e}^{-\frac{2}{\mathrm{n}}}\ldots\mathrm{e}^{-\frac{\mathrm{k}-1}{\mathrm{n}}}\right)=1-\mathrm{e}^{-\left(\frac{1}{\mathrm{n}}+\frac{2}{\mathrm{n}}+\ldots+\frac{\mathrm{k}-1}{\mathrm{n}}\right)}=1-\mathrm{e}^{-\frac{\mathrm{k}(\mathrm{k}-1)}{2\mathrm{n}}}. \quad (20)$$

Позначимо $P(n,k)=P_з$, тобто значенням ймовірності, з якої має виникнути колізія. В результаті маємо:

$$P_з=1-e^{-k(k-1)/2n},$$

або

$$1-P_з=e^{-k(k-1)/2n}. \quad (21)$$

Виконавши логарифмування (21), отримаємо:

$$\ln(1-P_з)=-k(k-1)/2n. \quad (22)$$

Перетворюючи (22), маємо:

$$\frac{k(k-1)}{2n}=-\ln(1-P_з)$$

або

$$\mathrm{k}\left(\mathrm{k}-1\right)=-2\mathrm{n}\ln\left(1-\mathrm{P}_з\right).$$

У кінцевому вигляді отримуємо:

$$\mathrm{k}^2-\mathrm{k}+2\mathrm{n}\ln\left(1-\mathrm{P}_з\right)=0. \quad (23)$$

У останньому рівнянні пов'язані три величини: число подій k, загальна кількість подій n та ймовірність P(n, k), з якою має виникати колізія. Знаючи відповідне значення $\mathrm{P}_з$ і n, можна отримати точне рішення щодо знаходження k.

Нехай $\mathrm{P}_з=0{,}5$, тоді з використанням (23) отримаємо:

$$\mathrm{k}^2-\mathrm{k}+2\mathrm{n}\ln 0.5=\mathrm{k}^2-\mathrm{k}-2\mathrm{n}\ln 2=0. \quad (24)$$

Якщо $\mathrm{n}=2^{\mathrm{m}}$, то рівняння (24) матиме вигляд:

$$\mathrm{k}^2-\mathrm{k}-2^{m+1}\ln 2=0. \quad (25)$$

Дамо оцінку значення k. З урахуванням (23), отримаємо:

$$\mathrm{k}^2=-2\mathrm{n}\ln\left(1-\mathrm{P}_з\right) \quad (26)$$

При $\mathrm{P}_з=0{,}5$, маємо:

$$\mathrm{k}^2=-2\mathrm{n}\ln\left(1-0{,}5\right)=2\mathrm{n}\ln 2.$$

Тоді оцінка k матиме значення:

$$\mathrm{k}=\sqrt{2\mathrm{n}\ln 2}\approx 1{,}41\sqrt{\mathrm{n}}. \quad (27)$$

Для довільного значення з рівняння (26) отримаємо:

$$k = \sqrt{2\ln\left(\frac{1}{1-P_3}\right)\cdot n} = 1,41\sqrt{\ln\left(\frac{1}{1-P_3}\right)\cdot n}\,. \qquad (28)$$

Співвідношення (28) дозволяє оцінити кількість перетворень (експериментів), які необхідно здійснити для виникнення колізії з ймовірністю $P_з$. Порівнюючи отримані для k значення ((27) - (28)) з оцінкою, яка наводиться в [6]:

$$k = \sqrt{n}\,, \qquad (29)$$

можна оцінити ступінь близькості оцінки та можливість її застосування.

Розглянемо приклад оцінки стійкості МАС. Нехай в якості H використовується хеш-функція SHA-1, в якій $n = 2^{160}$, і нехай: $P'_з = 0,5$ и $P''_з = 0,99$. Скориставшись виразом (28), отримуємо:

$$k_{0.5} = 1,41\sqrt{n} = 1,41\sqrt{2^{160}} = 1,41\cdot 2^{80} \approx 1,7\cdot 10^{24};$$

$$k = 1,41\sqrt{\ln\left(\frac{1}{1-0.99}\right)\cdot 2^{160}} = 2^{80} \approx 3\cdot 10^{24}.$$

Висновки

Таким чином, у роботі визначені типи атак на коди автентифікації повідомлень, у залежності від інформації, доступної зловмиснику. Сформульовані наукові підходи, отримані вирази, які дозволяють виконати оцінку стійкості МАС кодів при імітації та заміні. Показано, що для точного обчислення імітаційної та колізійної стійкості МАС кодів необхідно використовувати статистику спільних розподілів МАС кодів за ключами для дійсних та підроблених повідомлень. Доведено, що нижні межі для ймовірностей імітації та підміни не враховують статистичні властивості масивів автентифікаторів, і ґрунтуються на моделі псевдовипадковості функції f(x) та визначають мінімальні вимоги до розміру ключового простору та простору МАС значень, а верхні межі для ймовірностей імітації та підміни пов'язані з комбінаторними властивостями МАС масивів та оцінюють значення колізій у просторі МАС значень і повідомлень для найгіршого випадку вибору ключів та повідомлень. Розглянуті колізійні властивості МАС кодів. Отримані рівняння, які дозволяють точно розв'язати задачу визначення кількості експериментів (подій) k, які необхідно виконати для створення колізії з ймовірністю $P_з$ на безлічі значень МАС коду. Із застосуванням отриманих рівнянь виконані оцінки стійкості МАС для одного з типів хеш-функцій. Наведені у роботі результати дозволяють отримати як залежність числа подій k від значень ймовірності, з якої може виникнути колізія, і загальної кількості подій n, так і залежність ймовірності виникнення колізії від k і n.

Список літератури:

1. Gorbenko, I., Zamula, A., Ho, T.L., Rodionov, S. Derived Signals Systems for Information Communication Systems Applications: Synthesis, Formation, Processing and Properties 2020 IEEE International Conference on Problems of Info communications Science and Technology, PIC S and T 2020 – Proceedings this link is disabled, 2021, стр. 13–18, 9468058.

2. Gorbenko, I., Zamula, O. Devising Methods to Synthesize Discrete Complex Signals with required Properties for Application in Modern Information and Communication Systems. Eastern-European Journal of Enterprise Technologies this link is disabled, 2021, 3, стр. 16–26.

3. Gorbenko, I.D., Zamula, A.A. Information security and noise immunity of telecommunication systems under conditions of various internal and external impacts Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika), 2017, 76(19), стр. 1705-1717.

4. Gorbenko, I., Kudryashov, I., Malieieva, H. Comparative Analysis of Candidates for a Post-Quantum CPU Based on MQ Cryptographic Transformation. 2018 International Scientific-Practical Conference on Problems of Info communications Science and Technology, PIC S and T 2018 - Proceedings, 2019, стр. 442–446, 8632070.

5. Горбенко, І.Д. Прикладна криптологія. Монографія / І.Д. Горбенко, Ю.І. Горбенко. – Харків: ХНУРЕ, 2012 р. - 868 с.

6. Горбенко Ю.І. Побудова, аналіз, стандартизація та застосування криптографічних систем. Під загальною редакцією професора Горбенка І.Д. Харків.: Видавництво «Форт», 2015. – 959 с.

Надійшла до редколегії 10.01.2022

Відомості про авторів:

Горбенко Іван Дмитрович – д-р техн. наук, професор, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна, головний конструктор АТ «Інститут інформаційних технологій», Україна; e-mail: GorbenkoI@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-4616-3449

Замула Олександр Андрійович – д-р техн. наук, професор, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна, Україна; email: zamylaaa@gmail.com, ORCID: http://orcid.org/0000-0002-8973-6190