СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ
СИСТЕМЫ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ
SYSTEMS AND METHODS OF INFORMATION SECURITY

УДК 621.37: 004.056.5 **DOI:10.30837/rt.2021.4.207.14**

С.П. СЕРГІЄНКО, канд. фіз.-мат. наук, В.Г. КРИЖАНОВСЬКИЙ, д-р техн. наук,
Д.В. ЧЕРНОВ, канд. техн. наук, Л.В. ЗАГОРУЙКО, канд. техн. наук

ВИКОРИСТАННЯ НЕСТАЦІОНАРНИХ ШУМОВИХ ЗАВАД ДЛЯ ПРОТИДІЇ ПАСИВНИМ РАДІОЗАКЛАДКАМ

Вступ

В даний час інформаційна безпека розвивається в динамічній рівновазі між технологіями несанкціонованого зняття інформації і технологіями, що створюються для протидії такій діяльності. Для захисту від підслуховуючих пристроїв (радіозакладок) зазвичай використовуються системи радіопротидії, які встановлюють перешкоди в потенційно небезпечних для передачі інформації радіочастотних діапазонах або на частотах сигналів які щойно з'явилися [1, 2]. Такі перешкоди є шумовими сигналами, які іноді використовують ще й для потайної передачі інформації, для маскування переходу сигналу на іншу частоту [3 – 6], для прихованої передачі інформації шумові сигнали включаються між інформаційними пакетами [7]. Було показано, що застосування радіочастотного зашумлення не гарантує захисту приміщення від несанкціонованого зняття інформації при використанні пасивних радіозакладок [8 – 10]. Включення радіочастотного зашумлення може бути сигналом про те, що на території, яка захищається, відбуваються інформаційно цікаві події. Радіозакладка може використовувати енергію випромінювання генератора шуму для своєї активної роботи. До того ж такі радіозакладки можна зробити невидимими для існуючих в даний час таких засобів виявлення цих пристроїв, як нелінійні радіолокатори [11 – 14]. Екранування електронної схеми, а у відсутності радіозашумлення, відключення зв'язку електронної частини від антени – унеможливить виявлення радіозакладок. У той же час, включення радіо зашумлення створюватиме перешкоди для роботи нелінійного радіолокатора.

Для забезпечення скритності несанкціонованого підслуховування сигнали, які передаються радіозакладками, повинні мати малу потужність. Радіозакладки, що використовують для своєї роботи енергію зовнішнього радіочастотного випромінювання, принципово не мають достатнього потужного джерела енергії. Цим пояснюється мала відстань упевненого прийому сигналів радіозакладок. Забезпечити високу чутливість прийому слабких сигналів можна за допомогою приймачів, що накопичують енергію сигналу. Кореляційні приймачі мають перевагу в чутливості при прийомі сигналів, що передають малі обсяги інформації в одиницю часу. Накопичення енергії за час передачі біта інформації цифрового сигналу або за період часу максимальної частоти інформаційного аналогового сигналу забезпечує високу чутливість кореляційних приймачів.

В роботі [10] було отримано оптимальні режими роботи і розраховано параметри елементів схеми, які забезпечують ефективний режим роботи радіозакладки з використанням енергії радіочастотного зашумлення. В даній статті розглядається спосіб протидії радіозакладкам, які використовують для своєї роботи радіошумові сигнали, призначені для протидії підслуховуванню, за допомогою нестаціонарних шумів. Цей аналіз проводиться на прикладі використання кореляційних приймачів для реєстрації слабких сигналів. Вибір кореляційного приймача обумовлений тим, що для прийому випадкового радіочастотного сигналу кореляційний прийом є єдиним способом забезпечити прийнятну дальність впевненого прийому слабкого сигналу.

Основна частина

Модуляція радіочастотного зашумлення аналоговим акустичним або цифровим сигналом дозволяє налагодити канал витоку інформації [10]. Такий засіб підслуховування не потребує зовнішнього джерела енергії. Але інформаційний сигнал, що випромінює радіозакладка, має малу потужність, тому в якості приймача розглядаємо кореляційний приймач.

На схемі рис. 1 показана модель підслуховування з використанням енергії сигналу радіочастотного зашумлення, де 1 – генератор постановки радіочастотних завад, 2 – радіозакладка, 3 – антена прийому сигналу, який несе інформацію від радіозакладки, 4 – підсилювач інформаційного сигналу, 5 – антена опорного сигналу, направлена на генератор шумових завад, 6 – підсилювач опорного сигналу, 7 – блок нелінійного перетворення опорного сигналу, аналогічний тому, якому підвергається сигнал в радіозакладці, 8 – смуговий фільтр, смуга пропускання якого співпадає зі смугою випромінювання радіозакладки, 9 – перемножувач інформаційного та опорного сигналів, 10 – інтегратор. Сигнал, що надходить з радіозакладки, можна представити у вигляді: $U_1(t) = \mathrm{A}(t)U_0(t)$, де $\mathrm{A}(t)$ – інформаційний сигнал, спектр якого лежить в акустичному діапазоні, що модулює шумовий сигнал $U_0(t)$ спектр якого на багато порядків вище спектра сигналу $\mathrm{A}(t)$. У відсутності інформаційного сигналу при $\mathrm{A}(t) = 1$ на виході кореляційного приймача буде постійна напруга пропорційна потужності шумового сигналу. Сигнал, що надходить в опорний канал після проходження блоку нелінійного перетворення піддається аналогічному нелінійному перетворенню що і шумовий сигнал в радіозакладці. На виході з блоку 8 напруга $U_0(t)$ буде така ж, як і напруга в інформаційному каналі.

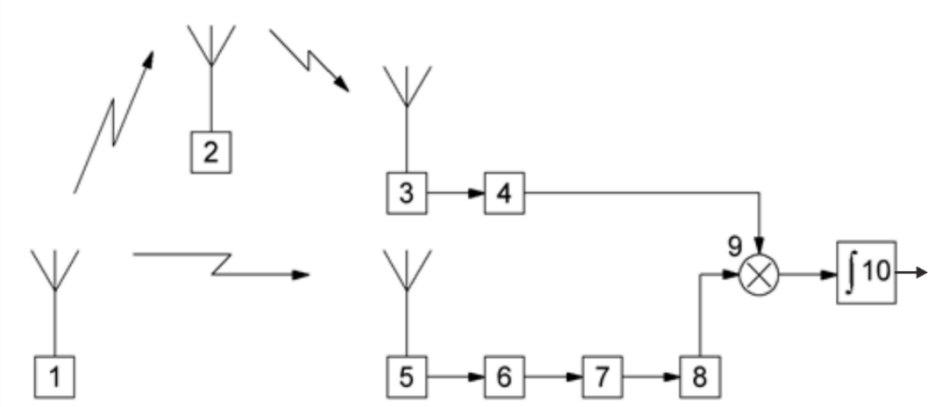


Рис. 1. Схема підслуховування з використанням енергії сигналу радіочастотного зашумлення

Сигнал на виході з кореляційного приймача (після перемножувача і інтегратора) визначається виразом $U(t) = \int_t^{t+\Delta t} U_1(t)U_0(t)^2 dt$, де $U_1(t) = \mathrm{A}(t)U_0(t)$. Інформаційний сигнал $\mathrm{A}(t)$ – функція, що повільно змінюється. За час інтегрування Δt, який визначається постійною часу інтегратора, можна вважати $\mathrm{A}(t)$ = const. При появі інформаційного сигналу він модулює шумовий сигнал. При передачі інформації сигнал на виході кореляційного приймача буде визначатися виразом

$$U(t) = \int_t^{t+\Delta t} \mathrm{A}(t)U_0(t)U_0(t)dt \cong \mathrm{A}(t) \int_t^{t+\Delta t} U_0(t)^2 dt. \quad (1)$$

Інтеграл $\int_t^{t+\Delta t} U_0(t)^2 dt$ (при відсутності амплітудної модуляції) буде константою, що не залежить від поточного часу t, якщо $U_0(t)$ буде стаціонарним випадковим сигналом, а $\Delta t >> \tau_0$, де τ_0 – час кореляції стаціонарного смугового випадкового сигналу. Цей інтеграл буде залежати від Δt. При модуляції шуму випадковий смуговий сигнал перестає бути стаціонарним і на виході перемножувача напруга буде змінюватися пропорційно інформаційному сигналу $\mathrm{A}(t) \int_t^{t+\Delta t} U_0(t)^2 dt$. Для часу інтегрування також повинна виконуватися друга умова

– $\Delta t < 1/f_m$, де f_m – максимальна частота в спектрі сигналу модуляції, або $\Delta t < T_b$, де T_b – час передачі одного біта інформації. Друга умова обмежує чутливість кореляційного приймача (збільшення Δt приведе к збільшенню інтеграла $\int_t^{t+\Delta t} U_0(t)^2 dt$ в виразі для вихідного сигналу (1)). Якщо час накопичування сигналу збільшити порівняно з умовою $\Delta t < 1/f_m$, при передачі аналогового сигналу буде втрачена частина спектральних складових інформаційного сигналу і інформаційний сигнал буде спотворений або, якщо не буде виконуватися умова $\Delta t < T_b$ при передачі цифрового сигналу, буде усереднена напруга логічної одиниці і логічного нуля і логічний перепад буде менше допустимого.

Спектр сигналу генератора перешкод для протидії роботі пасивних радіозакладок має вигляд, представлений на рис. 2. Розрахунки проводилися у відносних одиницях. Крива (a) – спектр потужності сигналу радіочастотних перешкод, (b) – спектр сигналу перешкод, який відбився від нелінійного елементу в підслуховуючому пристрої. Для активізації пасивної радіозакладки необхідне її опромінення електромагнітним випромінюванням досить великої амплітуди, здатної створити на нелінійному елементі напругу, амплітуда якої перевищує напругу термічного потенціалу $U = kT/q$. Тому пасивна радіозакладка буде більш ефективно працювати в безпосередній близькості джерела шумових перешкод і тому розташування генератора шумових перешкод біля радіопідслуховуючого пристрою не заважає його роботі, а, навпаки, збільшує дальність впевненого прийому інформації, що передається. Вузька смуга спектру радіочастотних перешкод обумовлена потребою уникнути негативного впливу на легальні радіопристрої. Зашумленню піддається частотний діапазон, в якому існує потенційна загроза несанкціонованого знімання інформації.

Для підвищення чутливості кореляційного приймача опорний сигнал повинен мати достатньо велику амплітуду. Для цього підсилювач 6 підвищує амплітуду опорного сигналу. Слід зазначити, рівень опорного сигналу, який надходить на антену 5, спрямовану на випромінюючу антену системи радіопротидії, набагато більший від інформаційного сигналу, який приходить на антену 3. Це обумовлено тим, що антену 5 кореляційного приймача можна зробити більш ефективною в порівнянні з антеною радіопідслуховуючого пристрою. Її габаритні розміри і конструкція не обмежені вимогами забезпечення скритності. На відміну від антени для підслуховування антена кореляційного приймача може мати вузьку діаграму спрямованості і у неї буде великий коефіцієнт посилення. Антена для підслуховування 2 менш ефективна в порівнянні з антеною 5, а перетворений сигнал буде ослаблений на нелінійному елементі радіопідслуховуючого пристрою. Тому, можна зробити висновок, що інформаційний сигнал на вході кореляційного приймача завжди буде значно слабше від опорного сигналу, прийнятого антеною 5. В інформаційному каналі сигнал набагато слабше в силу вище зазначених причин, тому він і визначає максимальну дальність прийому сигналу радіозакладки, обмежену шумами підсилювача, в нашому випадку це підсилювач 4 [10].

Розглянемо ефективність використання нестаціонарних шумових завад для протидії пасивним підслуховуючим пристроям. Можливість прийому сигналів в умовах присутності шумів з співпадаючим спектром аналізується за допомогою теорії [15], яка розроблена для аналізу забезпечення якісного прийняття шумоподібних радіосигналів в умовах присутності шумів, що заважають. Умови, щоб сигнал можна було розглядати як шумоподібний, визначаються співвідношенням, яке визначає базу шумоподібного сигналу $B = \Delta F \cdot T$, де ΔF – ширина смуги спектра сигнал. За умови, що $B > 1$ інформаційний сигнал можна вважати шумоподібним. У нашому випадку шумовий сигнал, модульований інформаційним сигналом, завідомо є випадковим і для нього також виконується співвідношення $B > 1$, тому ми можемо застосовувати, вищевказану теорію, для аналізу умови придушення каналу передачі інформації з радіозакладки, яка використовує шумові сигнали для передачі інформації. Завадостійкість прийому сигналу кореляційним приймачем залежить від співвідношення сигнал-шум на вході і бази сигналу B:

$$q^2 = 2B\rho^2, \tag{2}$$

де $\rho^2 = P_c/P_v$ – відношення потужностей сигналу і перешкоди. Завадостійкість зростає з ростом бази сигналу, інформація завжди передається сигналами відомої часової залежності, а завада носить випадкову залежність від часу. Тому збільшення часу накопичування або розширення спектру сигналу дозволяє виділити інформаційний сигнал змішаний с завадою. Оцінка завадостійкості береться виходячи з максимальності бази сигналу. Збільшити базу сигналу можна за рахунок збільшення ширини спектра і за рахунок збільшення тривалості сигналу. Змінити ширину спектру неможливо внаслідок того, що параметри шумового сигналу задаються системою захисту і зловмисники не можуть впливати на параметри системи радіопротидії. Збільшення база сигналу B за рахунок збільшення тривалості сигналу T призведе до зменшення швидкості передачі цифрової інформації, що часто неприпустимо через обмеженість часу, протягом якого актуальна передача інформації. Кількість біт інформації, переданої сигналом, у якого база сигналу була збільшена в T/T_0 разів, буде зменшена в стільки же разів. Тут T_0 – мінімальна тривалість часу передачі цифрової одиниці, яка пов'язана з максимальною частотою спектра сигналу згідно с теоремою Котельникова формулою $T_0 = 1/f_m$, f_m – максимальна частота спектра сигналу модуляції. Тому максимальна швидкість передачі інформації в одну секунду становить $1/T_0$.

Максимальна дальність прийому інформаційного сигналу визначається співвідношенням сигнал/шум в інформаційному каналі, що складається з шумів підсилювача і ефірних шумів. Рівність потужності шуму в спектральної смузі інформаційного сигналу і потужності інформаційного сигналу визначає максимальну дальність впевненого прийому сигналу. На вході перемножувача шум, присутній в опорному сигналі, набагато менше шуму в інформаційному сигналі і їм можна знехтувати. Сигнал на виході підсилювача 4 міститиме крім інформаційного сигналу ще й сигнал шуму підсилювача $V(t)$. Спектр шуму вважатимемо білим, пересічним зі спектром інформаційного сигналу.

$$U(t) = \int_t^{t+\Delta t}\{\mathrm{A}(t) + V(t)\}U_0(t)U_0(t)dt \cong \{\mathrm{A}(t) + V(t)\}\int_t^{t+\Delta t} U_0(t)U_0(t)dt. \tag{3}$$

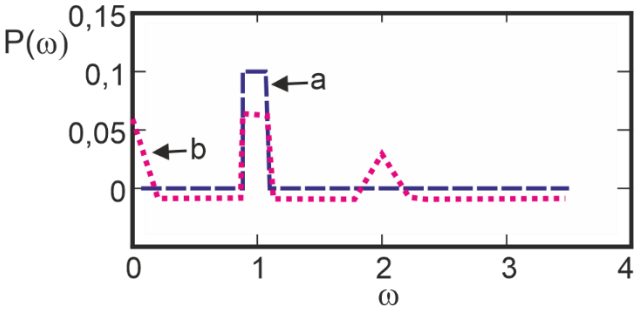
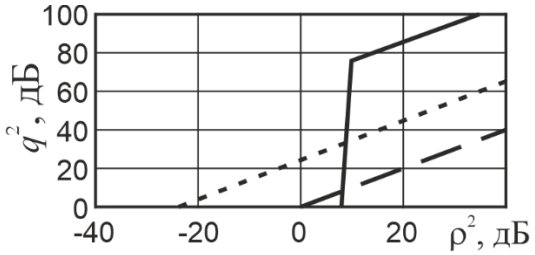


Рис. 2. Спектр сигналу генератора перешкод для протидії роботі пасивних радіозакладок (а) і спектр відбитого сигналу генератора перешкод від *p/n* переходу (b)



– – Амплітудна модуляція, – – – частотна модуляція, —— широкосмуговий сигнал

Рис. 3. Завадостійкість систем зв'язку за допомогою шумоподібних сигналів з різною модуляцією

Вважається що стійкість амплітудно-модульованого сигналу при однаковій базі B забезпечується при співвідношенні сигнал-шум $q^2\rho^2 = 1$ рис. 3 [15, с.7]). Рівень шуму в спектральній смузі частот інформаційного сигналу $U_0(t)$ можна зробити набагато більшим ніж спектральна потужність сигналу $A(t)$, що призведе до придушення каналу передачі інформації, який використовує енергію зашумлення в приміщенні. Для досягнення зазначеної мети необхідно провести амплітудну модуляцію шумового високочастотного сигналу (зашумлення) – шумом зі спектром акустичного діапазону. Сигнал зашумлення перестане бути стаціонар-

ним. На виході інтегратора, у якого постійна часу інтегрування $\Delta t < 1/f_m$, з'явиться шум $F_m(t)^2$, спектр якого буде перетинатися зі спектром сигналу модуляції $A(t)$. Розглянемо модуляцію випадкового високочастотного сигналу випадковим низькочастотним сигналом акустичного діапазону. Випадковий низькочастотний сигнал будемо описувати рядом Котельникова з максимальною частотою f_m. Сигнал на виході перемножувача

$$U = \int_t^{t+\Delta t} \mathrm{A}(t)F_m(t)U_0(t)F_m(t)U_0(t)dt \cong \mathrm{A}(t)F_m(t)^2 \int_t^{t+\Delta t} U_0(t)^2 dt \qquad (4)$$

де $U_0(t)$ – випадковий сигнал, що модулюється низькочастотним сигналом $F_m(t) = \sum_{-\infty}^{\infty} \xi_n \frac{\sin(t - n\frac{\pi}{\Omega})}{t - n\frac{\pi}{\Omega}}$, де ξ_n – випадкові амплітуди в відповідні моменти часу. Для забезпечення відсутності перемодуляції, випадкові амплітуди ξ_n повинні підкорятися рівномірному закону розподілу в діапазоні [-1,1]. При відсутності інформаційного сигналу $\mathrm{A}(t) = 1$ і спектр потужності сигналу на виході перемножувача описується виразом

$$P(\omega) = \int_{-\infty}^{\infty} e^{-i\omega\tau} \int_{-\infty}^{\infty} F_m(t)^2 F_m(t+\tau)^2 \, dtd\tau \qquad (5)$$

Графік спектру потужності на виході перемножувача представлений на рис. 4, крива (a). Спектр потужності на виході перемножувача ширше спектра низькочастотної обвідної модулюючого сигналу на вході перемножувача в обох каналах рис. 4, крива (b), тому можна модулювати шумовий сигнал випадковим сигналом з низькочастотним спектром, максимальна частота якого менше передбачуваного інформаційного сигналу. Спектр потужності сигналу на виході перемножувача при наявності інформаційного сигналу визначається виразом

$$P(\omega) = \int_{-T}^{T} e^{-i\omega\tau} \int_{-T}^{T} \mathrm{A}(t)F_m(t)^2 \mathrm{A}(t+\tau)F_m(t+\tau)^2 \, dtd\tau \qquad (6)$$

З огляду на те, що потужність шумової складової $|F_m(t)|^2$ значно перевищує потужність інформаційної складової $|\mathrm{A}(t)|^2$ вхідного сигналу перемножувача, неможливо відновити інформаційний сигнал (рис. 3). В якості ілюстрації було промодельовано передачу гармонійного сигналу радіозакладкою з використанням стаціонарного шуму. Спектр потужності на виході інтегратора для модуляції гармонічним сигналом $\mathrm{A}(t) = \sin\omega_0 t$ стаціонарного шуму визначається виразом

$$P_0(\omega) = \int_{-T}^{T} e^{-i\omega\tau} \int_{-T}^{T} \sin\omega_0 t \sin\omega_0(t+\tau) \, dtd\tau \qquad (7)$$

Вираз (7) є дельта функцією. Реальний сигнал проходить через інтегратор з кінцевим часом інтегрування T, рис. 5 (крива a). Час інтегрування брався рівним $200T_0$, де $T_0 = 2\pi/\omega_0$. На рис. 5 (крива b) представлено графік спектра потужності при модуляції монохроматичним сигналу нестаціонарного зашумлення при однаковому часі інтегрування. Потужність переданого монохроматичного сигналу при використанні нестаціонарного сигналу зашумлення набагато менше. Це обумовлено параметричною взаємодією корисного монохроматичного сигналу з модулюючим сигналом $F_m(t)$. Графік $N = 10log_{10}\left(\frac{P(\omega)}{P_{0(\omega)}}\right)$ на частоті $\omega = 1$ від часу усереднення T в (6) і (7) представлений на рис. 6. Завдяки використанню нестаціонарного шуму інформаційний монохроматичний сигнал послаблюється більш ніж 10 дБ порівняно з передачею такого ж сигналу стаціонарним шумом.

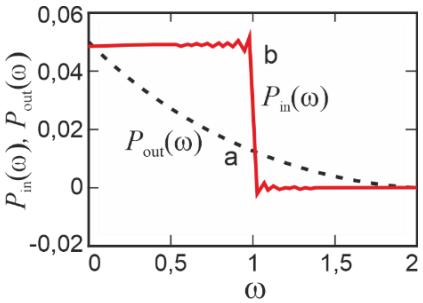


Рис. 4. Спектр потужності моделюючого сигналу на виході перемножувача (a) і на його вході (b)

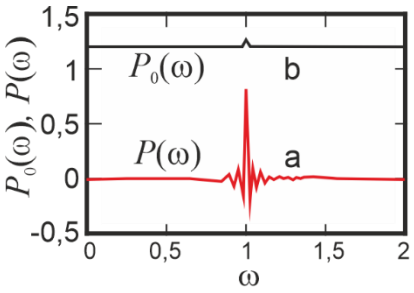


Рис. 5. Спектр потужності інформаційного гармонічного сигналу на виході корелятору при передачі сигналом зашумлення без модуляції (a) і з модуляцією (b)

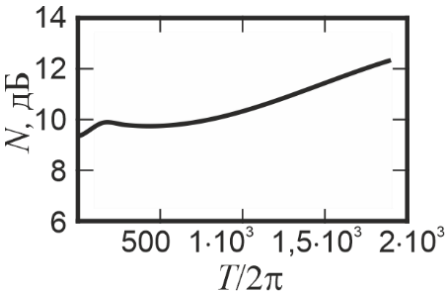


Рис. 6. Залежність послаблення інформаційного монохроматичного сигналу завдяки використанню нестаціонарного шуму від сталої часу корелятору

Висновки

Показано, що для протидії несанкціонованому зніманню інформації пасивними радіозакладками використання нестаціонарного шуму з випадковою 100 % амплітудною модуляцією в смузі частот сигналу, що передається, дозволяє подавити канал передачі інформації радіозакладок. Нестаціонарність шуму в діапазоні сигналу, що передається, призводить до його послаблення завдяки нелінійному перетворенню у перемножувачі кореляційного приймача. Використання вузькосмугових інформаційних сигналів для забезпечення прийнятного відношення сигнал/шум призведе до зниження швидкості передачі інформації, яка буде недостатня для передачі акустичної інформації в реальному масштабі часу.

Список літератури:

1. Encyclopedia of industrial espionage / Under total. ed. E. V. Kurenkova. St. Petersburg: ed. LLC "Publishing house Polygon", 1999. 515p.

2. Youhong Feng, Shihao Yan, Jinhong Yuan. User and Relay Selection With Artificial Noise to Enhance Physical Layer Security // Published 19 September 2018 Computer Science IEEE Transactions on Vehicular Technology. p. 10906-10920.

3. Xing H., Wong K., Chu, Z., Nallanathan A. To Harvest and Jam: A Paradigm of Self-Sustaining Friendly Jammers for Secure AF Relaying // IEEE Trans. Signal Process. 2015, 63, p. 6616–6631.

4. S. S. Kalamkar and A. Banerjee. Secure Communication via a Wireless Energy Harvesting Untrusted Relay // IEEE Transactions on Vehicular Technology, vol. 66, no. 3, pp. 2199-2213, March 2017.

5. Kyriakos Fytrakis, N. Kolokotronis, Konstantinos Katsanos, N. Kalouptsidis. Optimal Cooperative Strategies for PHY Security Maximization Subject to SNR Constraints Computer Science // IEEE Access 2020 DOI: 10.1109 / ACCESS.2020.3005481 Corpus ID: 220466452

6. Youhong Feng, Z. Yang, Shihao Yan, Nan Yang, Bin Lv It is shown that the JUFDRS scheme significantly outperforms the joint user and half-duplex relay selection (JUHDRS) scheme when the self-interference at the FD relay can be reasonably suppressed Computer Science // 2017 IEEE International Conference on Communications (ICC) 2017 TLDR DOI:10.1109/TVT.2018.2870280

7. C. Gong, X. Yue, Z. Zhang, X. Wang and X. Dai. Enhancing Physical Layer Security With Artificial Noise in Large-Scale NOMA Networks // IEEE Transactions on Vehicular Technology, vol. 70, no. 3, pp. 2349-2361, March 2021, doi: 10.1109/TVT.2021.3057661.

8. Serhiienko Sergey, Krizhanovski Vladimir, Chernov Dmitry. Transmission of Information by a Passive Radio Device in the Field of Radio Noise Interference with Transmission on Terrestrial Radio Frequency // Multidisciplinary Research. Abstracts of XIV International Scientific and Practical Conference Bilbao, Spain. December 21–24, 2020. P. 470–474. DOI – 10.46299/ISG.2020.II.XIV

9. Serhiienko S., Krizhanovski V. Modeling of the potential threat of unauth. orized removal of information by a passive radio tab in the rooms protected by noise field // The Fourth International Conference on Information and Telecommunication Technologies and Radio Electronic (UkrMiCo'2019) 09–13 September 2019 Odessa, Ukraine.

10. Serhiienko S.P., Kryzhanovsky V.G., Chernov D.V., Zagoruyko L.V. Effective modes of operation of radiocharging devices for secret recording of information in the field of noise interference // Radio Engineering. 2021. Vip. 205. S. 169-174. DOI:10.30837/rt.2021.2.205.18

11. A. S. Luchinin, I. V. Malygin, A. G. Dolmatov and A. A. Yazovsky. Synchronization and Noise Immunity of Communication Systems Using Signals with Multi-position Modulation // 2018Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), 2018, pp. 1-5, doi: 10.1109/SYNCHROINFO.2018.8456963.

12. Kyriakos Fytrakis, N. Kolokotronis, Konstantinos Katsanos, N. Kalouptsidis. Optimal Cooperative Strategies for PHY Security Maximization Subject to SNR Constraints Computer Science IEEE Access 2020 DOI: 10.1109 / ACCESS.2020.3005481 Corpus ID: 220466452

13. G. V. Kulikov, A. A. Lelyukh, E. V. Batalov, P. I. Kuzelenkov. Immunity of reception QAM signals in the presence of phase-shift keying interference // Radio electronics journal [electronic journal]. 2019. №7. Access mode: http://jre.cplire.ru/jre/jul19/10/text.pdf DOI 10.30898 / 1684-1719.2019.7.10

14. Alshammari A.S., Sobhy M.I., Lee P. (2018) Digital Communication System with High Security and High Noise Immunity: Security Analysis and Simulation. In: Barolli L., Xhafa F., Conesa J. (eds) Advances on Broad-Band Wireless Computing, Communication and Applications. BWCCA 2017. Lecture Notes on Data Engineering and Communications Technologies, vol 12. Springer, Cham. doi.org/10.1007/978-3-319-69811-3_43

15. Varakin L.E. Communication systems with noise-like signals, Moscow, P.384. https://www.studmed.ru/varakin-le-sistemy-svyazi-sshumopodobnymisignalami_7cfcca93721.html(accessed 14 May, 2019).

Надійшла до редколегії 10.10.2021

Відомості про авторів:

Сергієнко Сергій Петрович – канд. фіз.-мат. наук, доцент, Донецький національний університет імені Василя Стуса (м. Вінниця), доцент кафедри інформаційних технологій; Україна; email: s.serhiienko@donnu.edu.ua; ORCID: https://orcid.org/0000-0001-5515-8946

Крижановський Володимир Григорович – д-р техн. наук, професор, Донецький національний університет імені Василя Стуса (м. Вінниця), професор кафедри інформаційних технологій; Україна; email: v.krizhanovski@donnu.edu.ua; ORCID: https://orcid.org/0000-0002-2685-9740

Чернов Дмитро Вікторович – канд. техн. наук, Донецький національний університет імені Василя Стуса (м. Вінниця), доцент кафедри інформаційних технологій; Україна; email: d.chernov@donnu.edu.ua; ORCID: https://orcid.org/0000-0001-7173-0842

Загоруйко Любов Василівна – канд. техн. наук, Донецький національний університет імені Василя Стуса (м. Вінниця), доцент кафедри інформаційних технологій; Україна; email: l.zahoruiko@donnu.edu.ua; ORCID: https://orcid.org/0000-0002-6958-8696