РАДІОТЕХНІЧНІ СИСТЕМИ

УДК 621.391.82: 004.056.53 **DOI:10.30837/rt.2021.2.205.18**

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

ЕФЕКТИВНІ РЕЖИМИ РОБОТИ РАДІОЗАКЛАДНИХ ПРИСТРОЇВ ДЛЯ ПОТАЙНОГО ЗНІМАННЯ ІНФОРМАЦІЇ У ПОЛІ ШУМОВИХ ЗАВАД

Вступ

Відомі пасивні радіозакладні пристрої, які використовують для несанкціонованого зняття інформації [1], не мають джерела живлення. Такі пристрої використовують енергію зовнішнього джерела радіовипромінювання, рівень напруги яких перевершує термічний потенціал. Пристрій передає інформацію завдяки перетворенню частоти та енергії електромагнітних хвиль, якими вони опромінюються. Складовою частиною такого пристрою є елемент з нелінійною вольт-амперною характеристикою. Зазвичай таким елементом є високочастотний діод або пристрій з подібною вольт-амперною характеристикою. Нелінійність вольт-амперної характеристики $p-n$ переходу або діоду Штоки призводить до генерації коливань високочастотного поля на кратних частотах від частоти зовнішнього джерела опромінювання. Ефективне перетворення енергії високочастотного сигналу можливо при рівні сигналу на діоді від зовнішнього джерела опромінення, який перевищує напругу термічного потенціалу $kT/q = 0,26$ мВ. Частота інформаційного сигналу знаходиться в акустичному діапазоні спектру, що набагато менше ніж частоти електромагнітного опромінювання. Рівень генерації кратних гармонік залежить від зміщення робочої точки вольт-амперної характеристики $p-n$ переходу. Робоча точка зміщується напругою акустичного сигналу. Таким чином відбувається модульована по амплітуді генерація на кратних гармоніках частоти зовнішнього опромінювання. Використання шумового сигналу для забезпечення передачі інформації у різних варіантах пропонується в роботах [2, 3]. В [2] пропонується використовувати проміжний ретранслятор, який використовує енергію маскуючого зашумлення, що генерується зі сторони приймача системи передачі інформації. Зашумлення передається імпульсами, під час яких здійснюється передача від передавача до проміжного ретранслятора і накопичення енергії від сигналу зашумлення в ретрансляторі, а в паузах зашумлення інформація передається від ретранслятора до приймача. Для підтримки такого режиму роботи ретранслятор має дві направлені антени, спрямовані до передача та приймача.

В роботі [3] досліджується безпека фізичного рівня кооперативного неортогонального множинного доступу NOMA (Non-Orthogonal Multiple Access) в жорсткому сценарії, де немає прямого зв'язку від джерела до дальнього пункту призначення, в той час як прямий зв'язок між пристроєм підслуховування і джерелом існує. Для забезпечення безпеки зв'язку в цьому сценарії пропонується схема кооперативного неортогонального множинного доступу з використанням глушіння. Зокрема, глушильний пристрій може пасивно збирати енергію оточуючих джерел радіочастотних сигналів, а зібрана енергія використовується для випромінювання шуму, щоб не дозволити підслуховування. Доданий шум змінює локальний рівень сигналу. Завдяки цьому зовнішній пристрій, що підслуховує, не зможе по рівню потужності визначити адресу призначення інформації.

Для боротьби з несанкціонованим зніманням інформації за допомогою пасивних радіозакладок використовують генератори шуму [4 – 6]. Генератори шуму випромінюють в потенційно небезпечному діапазоні частот радіохвилі, їх рівень потужності перевершує потужність генерації радіозакладного пристрою. Зашумлення об’єктів, що підлягають захисту, у всьому можливому на даний час діапазоні частот технічно складно, і це також призводить до

унеможливлення нормальної роботи систем радіозв'язку навколо об'єктів, що захищаються. Більш прийнятним є захист з використанням зашумлення на деяких вузьких частотних діапазонах, на яких є загроза передачі інформації радіозакладними пристроями. Це може бути на діапазонах роботи стільникового зв'язку, або в діапазоні, в якому починає роботу радіопередавальний невідомий пристрій та рівень випромінювання якого достатній для активізації радіозакладних пристроїв [7]. Потенційно небезпечно передавати інформацію за допомогою NFC-зв'язку. Зловмисники можуть несанкціонованим чином зняти інформацію на кратних гармоніках [8]. Для протидії такому витоку інформації можливо використовувати зашумлення на частотах кратних частоті передачі інформації NFC-зв'язку 13,65 МГц. Такий захист значно простіше використовувати, так як ці діапазони відносяться до промислових частот і тому він не буде заважати роботі інших користувачів.

В статті демонструється можливість роботи радіозакладного пристрою з використання енергії генератору шуму, який повинен заважати несанкціонованому зніманню інформації. Схема, в якій можливе потенційне знімання інформації з використанням генератору шуму, представлена на рис. 1, де: ПП – пристрій, що підслуховує; ФНЧ – фільтр низьких частот; ГШ – генератор шуму для протидії підслуховуванню; ПВЧ – приймач високих частот; ПНЧ – приймач низьких частот. Інформація може передаватися по високочастотних і низькочастотних каналах.

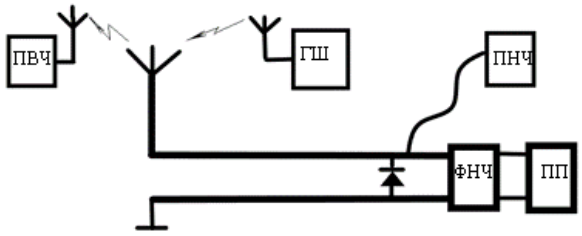


Рис. 1

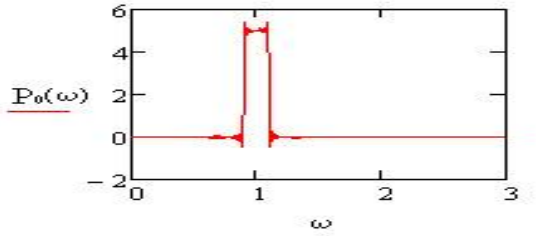


Рис. 2

Моделювання нелінійних перетворень спектру шумових завад

Моделювання потенційної можливості знімання інформації в полі шумових завад ГШ (рис. 1) проводиться на спрощеній моделі [9]. Радіозакладка моделюється діодом, який підключено до кінця довгої лінії з хвильовим опором Z_0. До лінії передачі з іншого кінця підключена широкосмугова антена. Шумовий сигнал модулюється Гаусовим смуговим сигналом зі спектром, як на рис. 2, частота ω – це нормована частота на центральну частоту діапазону.

Для радіозакладних пристроїв частіше використовується дециметровий діапазон радіохвиль. Вибір цього діапазону зумовлений тим, що розмір антени повинен бути невеликим, щоб не викривати скритність пристрою і забезпечити можливість безперешкодного розповсюдження інформаційного сигналу в умовах приміщень. Частота інформаційного акустичного сигналу не перевершує 10 кГц. Після змішення випадкової напруги шумового сигналу з інформаційним акустичним сигналом на нелінійному елементі випадковий сигнал змініть свій спектр і перестане бути ергодичним. Інформація буде закодована в амплітудну модуляцію шумового сигналу.

Рівняння, яке описує зв'язок напруги падаючої хвилі U_F від ГШ, параметри лінії передач (хвильовий опір Z_0), з напругою і струмом нелінійного елемента та напругою відбитої хвилі U_R, має вигляд (1) [10]. Це рівняння справедливо для безінерційного нелінійного перетворення. Таке наближення справедливо в разі, якщо частота сигналу і постійна часу τ знаходяться в співвідношенні $\omega \ll 1/\tau$. Стала τ визначається хвильовим опором лінії Z_0 і ємністю $p-n$ переходу C і дорівнює $\tau = Z_0 C$. Напруга на кінці довгої лінії буде складатися з напруги

падаючої хвилі U_F, напруги відбитої хвилі U_R і напруги зміщення U_0, яка модулює опір діоду:

$$U = U_0 + U_F + U_R. \tag{1}$$

Зв'язок між напругами падаючої хвилі, відбитої хвилі та струмом на кінці довгої лінії і хвильовим опором описується виразом [10]

$$U_F - U_R = I \cdot Z_0. \tag{2}$$

В якості навантаження на кінці довгої лінії встановлено діод, його вольт-амперну характеристику будемо вважати ідеалізованою з експоненціальною залежністю струму від напруги. Враховуючи (1) і (2), отримаємо

$$U_F - U_R = j_0\left(e^{\frac{q(U_0+U_F+U_R)}{kT}} - 1\right)Z_0. \tag{3}$$

З рішення рівняння (3) відносно U_R отримаємо залежність напруги відбитої хвилі $U_R\left(U_F, U_0, Z_0\right)$. Падаючу хвилю (шумовий сигнал, який використовується для протидії несанкціонованому зніманню інформації) описуємо випадковим сигналом з Гаусовим розподілом амплітуди і смуговим спектром. Кореляційна функція такої такого сигналу описується [11] так:

$$r(\tau) = \frac{\sin \Delta\omega\tau \cdot \cos \omega_0\tau}{\pi\Delta\omega\tau}. \tag{4}$$

Спектральна щільність потужності падаючої хвилі

$$P_0(\omega) = \int_{-\infty}^{\infty} r(\tau) e^{-i\omega\tau} d\tau. \tag{5}$$

Графік спектральної щільності потужності падаючої хвилі представлений на рис. 2. Кореляційна функція відбитої хвилі визначається формулою (6); в такому вигляді кореляційна функція нормована на опір довгої лінії з приєднаним нелінійним елементом. Спектр відбитої хвилі находиться заміною $r(\tau)$ на $B(\tau)$ у формулі (5):

$$\begin{aligned} B(\tau) = \int_{-\infty}^{\infty}\int U_R\left(U_{F1}, U_0, Z_0\right) U_R\left(U_{F2}, U_0, Z_0\right) \frac{e^{\frac{-\left(U_{F1}^2 + U_{F2}^2 - 2U_{F1}U_{F2}r(\tau)\right)}{2\sigma^2\sqrt{1-r(\tau)^2}}}}{Z_0 \cdot 2\pi\sigma\sqrt{1-r(\tau)^2}} dU_{F1} dU_{F2} - \\ - \frac{1}{Z_0}\left(\int_{-\infty}^{\infty} \frac{U_R\left(U_F, U_0, Z_0\right) e^{\frac{U_F^2}{2\sigma^2}}}{\sqrt{2\pi\sigma}} dU_F\right)^2 \end{aligned} \tag{6}$$

Спектральна щільність потужності відбитої хвилі для напруги зміщення $U_0 = 3$ і опору довгої лінії $Z = Z_0/\left(kT/qj_0\right) = 1$ має вигляд, представлений на рис. 3. Взаємне співвідношення максимумів спектральної щільності поблизу частот $\omega = 0$, $\omega = 2$ та $\omega = 1$ змінюється в протилежних напрямках в залежності від опору довгої лінії і напруги зміщення. Якщо спектральна щільність поблизу частот $\omega = 0$, $\omega = 2$ збільшується, то спектральна щільність поблизу частоти $\omega = 1$ зменшується, і навпаки. На відмінність від спектральної щільності потужності шумового сигналу який використовується для протидії несанкціонованого зніманню інформації (рис. 2), хвиля, відбита від нелінійного елемента, має у спектру потужності складові, які відсутні у шумовому сигналі падаючої хвилі. Залежність потужності відбитої хвилі від дисперсії шумового сигналу на подвійної частоті і при напрузі $U_0 = -3$ представлена на рис. 4. Потужність відбитої хвилі зростає за експоненціальним законом від дисперсії шуму.

На рис. 5 представлена залежність спектральної щільності потужності від сталої напруги, прикладеної до нелінійного елемента. Розрахунок проводився для опору $Z = 0{,}1$. Вибір опору був обумовлений тим, що зміна напруги зміщення в Вольтах від $+3kT/q$ до $-9kT/q$ призводить до збільшення діапазону зміни диференційного опору діоду, що відображається на кількості максимумів і співвідношенні висот максимумів спектральної щільності. Як видно з графіку, зміна спектральної щільності в залежності від напруги зміщення носить немонотонний характер. Найбільшій рівень нелінійних перетворень спектру відбитої хвилі спостерігається при прямому зміщенні діоду.

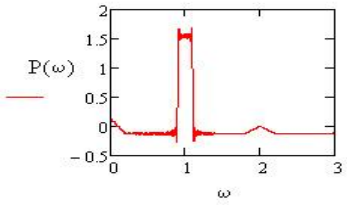


Рис. 3

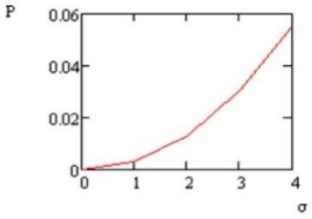


Рис. 4

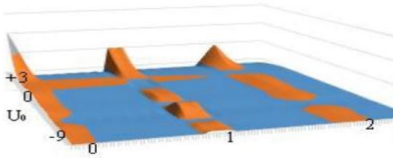
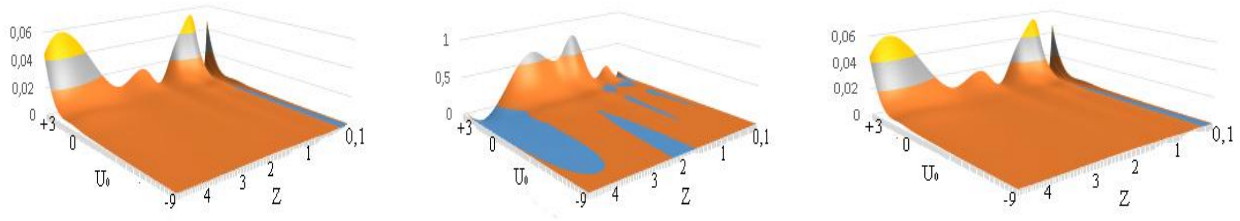


Рис. 5

Для несанкціонованого знімання інформації більш привабливими є спектральні складові відбитої хвилі, які групуються біля нульової частоти та біля подвійної частоти $2\omega_0$ завдяки більшої потужності цих складових, та відсутності в цих діапазонах сигналу зашумлення. Використання частот біля нульової частоти більш привабливе для передачі інформації через провідні лінії електропередачі, металеві елементи будівельних конструкцій, металеві елементи водо-теплопостачання, каналізаційні споруди, тощо. Для передачі інформації через ефір більш підходить спектральний максимум біля частоти $2\omega_0$, де ω_0 – центральна частота смуги зашумлення. В такому випадку простіше забезпечити ефективний прийом та передачу однією антеною на відміну від використання спектральних складових на частотах $3\omega_0$ та вище. Ефективність нелінійного перетворення шумового сигналу залежить від двох параметрів: напруги зміщення, що подається на діод та опору довгої лінії (точніше відношення опору лінії до диференціального опору діоду без зміщення. Диференційний опір діоду при розрахунках без напруги зміщення береться в безрозмірних одиницях $Z_d = Z_0/(kT/qj_0)$ де Z_0 хвильовий опір довгої лінії. $Z_d = 1$ буде в випадку підключення до довгої лінії діоду зі $j_0 \cong 2\cdot 10^{-3}$ А. Ефективність перетворення випадкового сигналу падаючої хвилі буде залежати від рівня сигналу шуму σ, та співвідношення хвильового опору Z_0 та диференційного опору діоду $(kT/qj_0)e^{(qU_0/kT)}$.

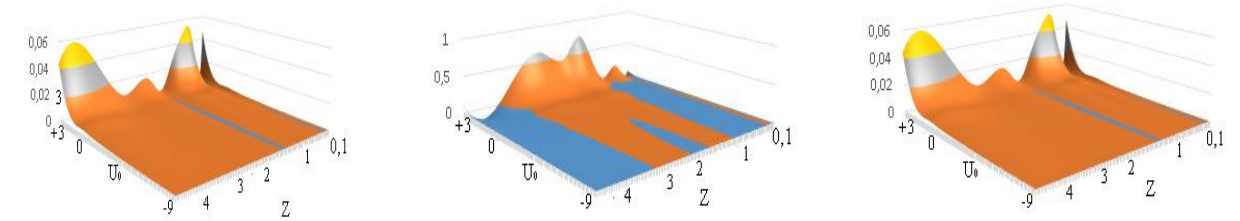
Всі розрахунки велися для рівня дисперсії генератору шуму $\sigma = 3$. Дисперсія виміряється в одиницях термічного потенціалу. Диференційний опір залежить від напруги, яка зміщує робочу точку вольт-амперної характеристики діоду U_0. Таким чином, змінюючи напругу U_0, теоретично можливо змінювати опір діоду від 0 до ∞. Рівень корисного сигналу від пасивної радіозакладки низький порівняно з активними радіозакладними пристроями. Тому для збільшення відстані, на якій можливий впевнений радіоприйом, треба використовувати широкосмугові приймачі. Моделювання такого прийому проводилося з урахуванням енергії відбитої хвилі на всій смуги низькочастотного максимуму $P_0(U_0, Z) = \int_0^{2\Delta\omega} W(\omega, U_0, Z)d\omega$; на спектральному максимумі на частоті падаючої хвилі $P_1(U_0, Z) = \int_{\omega_0-\Delta\omega}^{\omega_0+\Delta\omega} W(\omega, U_0, Z)d\omega$ та максимумі біля подвійної частоті від центральної частоти падаючої хвилі $P_2(U_0, Z) = \int_{2\omega_0-\Delta\omega}^{2\omega_0+\Delta\omega} W(\omega, U_0, Z)d\omega$. Залежність потужностей відбитої хвилі на різних максимумах спектральної щільності від напруги зміщення і хвилевого опору представлена на рис. 6, *а* – $P_0(U_0, Z)$, на рис. 6, *б* – $P_1(U_0, Z)$, на рис. 6, *в* – $P_2(U_0, Z)$.



а *б* *в*

Рис. 6

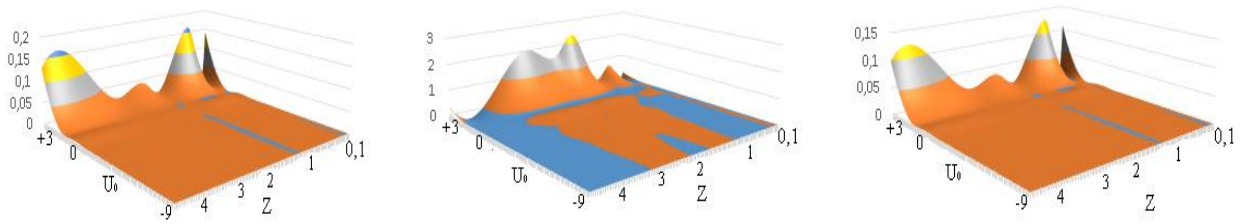
Для передачі інформації можливо використовувати два режими. Бінарний – це коли управляюча напруга приймає два значення. В цьому випадку вибираються два значення напруги, які зміщують робочу точку таким чином, щоб забезпечити максимальну різницю потужності перетвореного сигналу у вибраному діапазону частот. Цей режим більш відповідає передачі інформації цифровим сигналом. Ефективність бінарного режиму модуляції визначається максимумом різниці спектральної щільності потужності при прикладенні до діоду напруги зміщення $P(U_0, Z)$ (умовна логічна одиниця) та при прикладенні зворотної напруги зміщення $P(-9, z)$ (умовний логічний нуль). Передача інформації буде більш надійнішою, якщо логічний перепад $\Delta P_{\text{і}}(U_0, Z) = P_{\text{і}}(U_0, Z) - P_{\text{і}}(-9, Z)$ буде максимальним. Залежність потужності $\Delta P_{\text{і}}(U_0, Z)$ від U_0 і Z представлено на рис. 7. Опір довгої лінії представлений в відносних одиницях $(kT)/(qj_0)$. В $\Delta P_{\text{і}}(U_0, Z)$ різні індекси відноситься до різних максимумів спектральної щільності. На рис. 7, *а* зображена залежність $\Delta P_0(U_0, Z)$ спектральної щільності потужності біля нульової частоти. Відповідно залежність $\Delta P_1(U_0, Z)$ спектральної щільності потужності біля частоти ω_0 – на рис. 7, *б*, а залежність $\Delta P_2(U_0, Z)$ спектральної щільності потужності частоти біля частоти $2\omega_0$ – на рис. 7, *в*.



а *б* *в*

Рис. 7

Другий режим передачі інформації більш придатний для передачі аналогової інформації. В цьому режимі управляючий сигнал складається з двох компонентів – зі сталої напруги, яка переміщує робочу точку у діапазон, в якому диференційна характеристика перетворення енергії падаючої хвилі буде більшою, та змінної напруги, якою є акустичний сигнал. Було получено диференційну залежність спектральної потужності від напруги U_0 та опору довгої лінії Z. На рис. 8 представлено залежність $\left|\frac{\partial P_i(U_0,Z)}{\partial U_0}\right|$ від напруги зміщення та різних опоров довгої лінії. Похідна береться поблизу максимумів біля частот 0, ω_0 і $2\omega_0$.



а *б* *в*

Рис. 8

Ефективність двох режимів найбільша при роботі в режимі прямого зміщення діоду. Залежності $\Delta P_{\text{і}}(U_0, Z)$, яка відповідає бінарному режиму модуляції, і $\frac{\partial P_i(U_0,Z)}{\partial U_0}$, яка відповідає аналоговому режиму модуляції від опору довгої лінії, мають немонотонний характер з декількома максимумами. Аналоговий режим модуляції має більшу ефективність, якщо хвильовій опір довгої лінії буде менший за опір нелінійного елемента, на якому відбувається перетворення шумового сигналу. Це справедливо для всіх трьох максимів спектральної щільності.

Висновки

Показано, що пасивний радіозакладний пристрій з використанням нелінійного елемента в полі радіошумових перешкод може передавати інформацію з використанням енергії цих радіошумових завад. Показана можливість та запропоновано режими передачі аналогової та цифрової інформації. Рівень сигналу завдяки нелінійному перетворенню енергії вузькосмугового сигналу радіоперешкод більший при прямому зміщенні діоду. Показано, що передача аналогового та бінарного сигналу в режимі амплітудної модуляції по високочастотному і низькочастотному каналах більш ефективна при прямому зміщенні діоду для співвідношення опорів діоду Z_d і довгої лінії $Z = Z_d/2$ і $Z = 4Z_d$. Передача інформації бінарним і аналоговим сигналом в смузі частот поблизу максимумів ω_0 ефективна для співвідношення опорів $3{,}5Z_d \geq Z \geq 2{,}5Z_d$.

Список літератури:

1. Энциклопедия промышленного шпионажа ; под общ. ред. Е.В. Куренкова. С.-Петербург : ООО «Изд-во Полигон», 1999. 515с.
2. Kalamkar S. S. and Banerjee A. Secure Communication via a Wireless Energy Harvesting Untrusted Relay // IEEE Transactions on Vehicular Technology. March 2017. Vol. 66, no. 3. P. 2199-2213,
3. Cao et K. al. Energy Harvesting Jammer Enabled Secure Communication for Cooperative NOMA Systems // 2020 International Conference on Wireless Communications and Signal Processing (WCSP), 2020. P. 801-806
4. United States Patent 8665607 Bouza, et al. Anti-eavesdropping device. H05K 7/14; H05K 7/18, March 4, 2014
5. Емельянов С. и др. Проблемные аспекты реализации пространственного и линейного зашумления в системах активной защиты информации // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Харків, 2001. Вип. 2. С. 62-67.
6. Петров А.А. Оценка эффективности систем активной защиты в сетях общего пользования // Системы обробки інформації. Харьков, 2011. №4(94). С.174-178.
7. Патент РФ № 2732486 Способ радиоподавления систем когнитивных систем радиосвязи. Бюл. № 26 17.09.20.
8. Крижановський В.Г., Сергієнко С.П., Чернов Д.В., Крижановський В.В. Підслуховування NFC-зв'язку на частотах вищих гармонік // Радіотехніка. 2021. Вып. 204. С. 99-104.
9. Serhiienko S., Krizhanovski V. Modeling of the potential threat of unauthorized 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. Нейман Р.Л., Демирчан К.С. Теоретические основы радиотехники. Т.1. Ленинград : Энергоиздат, 1981. 536с.
11. Баскаков С.И. Радиотехнические цепи и сигналы. Москва : Высш. шк., 1983. 536с.

Надійшла до редколегії 09.03.2021

Відомості про авторів:

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

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

Чернов Дмитро Вікторович – канд. техн. наук, Донецький національний університет імені Василя Стуса (м. Вінниця), доцент кафедри радіофізики та кібербезпеки; 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 радіофізики та кібербезпеки; Україна; email: l.zahoruiko@donnu.edu.ua; ORCID: https://orcid.org/0000-0002-6958-8696