DOI: 10.35681/1560-9189.2022.24.2.275041

УДК 004.2.056.55

Д. В. Євграфов, Ю. Є. Яремчук
Вінницький національний технічний університет
Хмельницьке шосе, 95, 21021 Вінниця, Україна

Розподілення амплітуди шумового генератора для придушення побічних електромагнітних випромінювань з екрана монітора

Розглянуто структуру сучасного широкосмугового шумового генератора для боротьби з побічними електромагнітними випромінюваннями та наведеннями, який генерує випадковий цифровий код і перетворює його на безперервний сигнал. Досліджено вплив сигналу генератора на ймовірність хибної тривоги технічного засобу розвідки противника, узгодженого з сигналом побічних випромінювань і наведень з екранів моніторів на рідинно-кристалічних структурах. Доведено, що вплив пропорційний дисперсії шумового сигналу. Приведено дослідження сигналу віброакустичного генератора шуму «Марс» у програмному продукті Excel, за структурою схожого на сучасний шумовий генератор для боротьби з побічними електромагнітними випромінюваннями. У припущенні, що сигнал ідеального шуму близький до рівномірно розподіленого, знайдено подання розподілення амплітуди рядом з парними поліномами Лежандра першого роду. Показано, що в разі ускладнення розрахункової задачі пошуку випадкових кодів їх можна замінити гармоніками з дискретними рівномірно розподіленими фазами або дискретними рівномірно розподіленими випадковими величинами.

Ключові слова: *побічні електромагнітні випромінювання та наведення, монітори на рідинно-кристалічних структурах, білий гаусівський шум, системи ортогональних поліномів, поліноми Лежандра першого роду.*

Вступ

Сучасні способи генерування шумового сигналу для активного захисту інформації від витоку через побічні електромагнітні випромінювання і наведення (ПЕМВІН) потребують розуміння того, що змінилося з часів переходу на цифрові технології генерування шумових сигналів.

Припустимо, що нам треба створити генератор шуму (ГШ) активного захисту інформації від витоку через ПЕМВІН, що складається з мікропроцесорної системи

© Д. В. Євграфов, Ю. Є. Яремчук

(МПС) для генерації випадкових цифрових кодів i , $i = 1,...,2^M$, *М*-розрядного цифро-аналогового перетворювача (ЦАП) і фільтра низької частоти (ФНЧ), поданого на рис. 1.

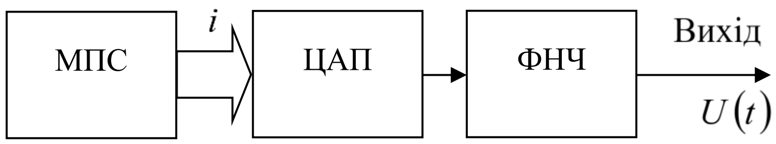


Рис. 1. Структура сучасного ГШ для боротьби з ПЕМВІН

Продуктивність сучасних МПС дозволяє створювати випадкові цифрові послідовності з періодами дискретизації $T_д \geq 0,7 \cdot 10^{-10}$ с [1], які після перетворення в ЦАП і ФНЧ в напругу $U(t) \in [-U_{\max}, U_{\max}]$, $U_{\max}$ — максимальне значення напруги ГШ, ефективно придушують ПЕМВІН у смузі частот від мінімальної $F_{\min}$ до максимальної $F_{\max}$, забезпеченими відповідно до теореми Шенона-Котельникова для $T_д \leq 1/[2(F_{\max} - F_{\min})]$. Отже, потенційні можливості сучасної МПС дозволяють створювати ГШ із заданими спектральними характеристиками, ефективні спектри яких $\Delta F = F_{\max} - F_{\min}$ сягають до 7 ГГц!

Коли як джерело випадкового сигналу ГШ використовувалися напівпровідникові елементи, розподілення амплітуд їхніх безперервних реалізацій вважалися гаусівськими, а для оцінювання якості шуму застосовувалися коефіцієнти, які характеризували їхню близькість до гаусівсько-розподілених випадкових величин [2]. Це не було наслідком обґрунтування «ідеальності» гаусівського шуму, а витікало із можливостей кінця 80-х років генерувати широкосмугові випадкові сигнали [3, 4].

На той час:

— способи генерування безперервних широкосмугових шумових сигналів не передбачали іншого розподілення амплітуд, крім гаусівського;

— було розроблено математичну теорію двовимірних гаусівських процесів і їхню ідеалізацію у вигляді білого гаусівського шуму (БГШ);

— усі наявні методики оцінювання якості ГШ були спрямовані на порівняння їхніх параметрів з гаусівськими, тому що не існувало інструментарію оцінювання розподілень шумових сигналів, відмінних від гаусівських.

Отже, в задачах генерування шумових сигналів раніше не розглядали питання розподілення їхніх амплітуд. Якщо «шуму не вистачало» просто збільшували його потужність (дисперсію гаусівсько-розподіленої амплітуди). Але, коли йдеться про сучасні цифрові технології генерування шумового сигналу у вигляді нап-руги $U(t)$, обмеженої інтервалом $[-U_{\max}, U_{\max}]$, можна поставити та розв’я-зати задачу пошуку розподілення амплітуди в зазначеному інтервалі амплітуд, що в кращій спосіб придушуватиме витік інформації.

Постановка задачі

Розглянемо ГШ, який не змінює своїх енергетичних характеристик у рівномірному спектрі частот від $F_{\min}$ до $F_{\max}$. Припустимо, що в системі захисту інформації від витоку із засобу обчислювальної техніки (ЗОТ) він наводить в антенній системі технічного засобу розвідки (ТЗР) противника сигнал $U_{ш\ пр}(t)$, а ЗОТ — сигнал $U_{с\ пр}(t)$, що подано на рис. 2.

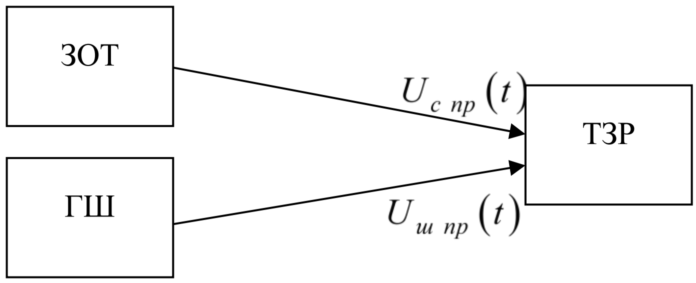


Рис. 2. Система захисту технічного каналу витоку інформації

Знехтуємо природніми й індустріальними перешкодами і вважатимемо, що на виході антенної системи ТЗР напруга дорівнюватиме: $U_{с\ пр}(t)+U_{ш\ пр}(t)$. Припустимо, також, що антенна система на виході ГШ і середовище поширення радіохвиль від ГШ до ТЗР мінімально перетворюють спектр сигналу (крім, зрозуміло, постійної складової) таким чином, що

$$U_{ш\ пр}(t)=\gamma U(t), \tag{1}$$

де γ — деяка константа, яка залежить від концентрації електромагнітної енергії (ЕМЕ) антенними системами ГШ і ТЗР, а також від процесів згасання ЕМЕ у просторі; $U(t)$ — сигнал на виході ГШ.

Нехай ідеться про протидію витоку інформації з екрана монітора на рідинно-кристалічних структурах ЗОТ, на екрані якого протягом часу аналізу T_a не змінюється картинка, а противнику відома частота кадрової розгортки монітора $f_к$. У цьому випадку ТЗР накопичує сигнали витоку інформації $U_{с\ пр}(t)$ у лінійній системі з гребеневою амплітудно-частотною характеристикою, центральні частоти гребенів якої відстають одна від одної на $f_к$, а ширина кожного гребеня дорівнює $1/T_a$ (див. рис. 3) [5].

Виявлювач сигналу ПЕМВІН складається із гребеневого фільтра (ГФ), детектора огинаючої (ДО) і порогового пристрою (ПП). Рішення про наявність ПЕМВІН приймається, коли сигнал перевищує деякий поріг виявлення *h*, а ймовірність хибної тривоги сигналу ПЕМВІН дорівнюватиме:

$$F = \int_{h}^{\infty} w_0(y)\,dy\,, \tag{2}$$

де $w_0(y)$ — густина ймовірності розподілення сигналу $y(T_a)$, коли у вхідній реалізації сигналу ПЕМВІН немає.

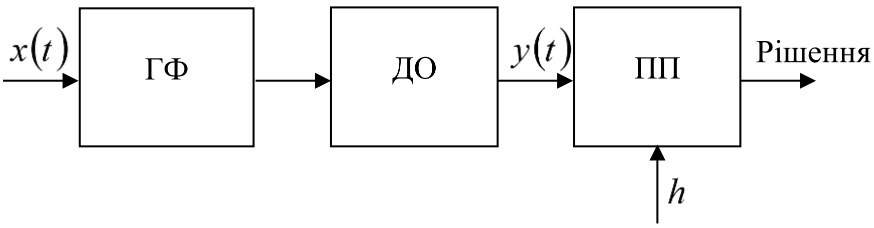


Рис. 3. Структура ТЗР як виявлювача сигналу ПЕМВІН

Лінійний тракт ТЗР – ГФ являє собою $n = \Delta F \,/\, f_к$ смугових фільтрів з шириною перепускання $1/T_a$, загальна смуга перепускання яких приблизно дорівнюватиме $\Delta f \approx \Delta F \,/\, f_к T_a$. Коли ЗОТ вимкнений, і внутрішній шумовий процес ТЗР незалежний від сигналу ГШ, сигнал перед ДО є фактично реакцією вузькосмугової лінійної системи на зовнішній і внутрішній шуми, яка розподілена за центрованим гаусовським законом із дисперсією

$$\sigma^2 = \frac{1}{f_к T_a}\left(\gamma^2\sigma_ш^2 + N_0\Delta F\right), \tag{3}$$

де $\sigma_ш^2$ — дисперсія випадкового сигналу $U(t)$; N_0 — однобічна спектральна густина потужності білого гаусівського шуму (БГШ) приймача ТЗР. Тому густина ймовірності розподілення процесу на виході ДО $w_0(y)$ має релеєвський характер, а ймовірність хибної тривоги (2) можна розрахувати за виразом

$$F = \exp\left(-\frac{h^2}{2\sigma^2}\right). \tag{4}$$

Імовірність (4) тим більша для фіксованого *h*, чим більшою є дисперсія (3), а для фіксованих N_0, $f_к, T_a$, які не залежать від параметрів ГШ, якість генерованого шумового сигналу тим краща, чим більшим є добуток $\gamma^2\sigma_ш^2$.

Мета роботи: обґрунтувати розподілення випадкового стаціонарного процесу на виході ГШ $U(t)$, $U(t) \in [-U_{\max}, U_{\max}]$, яке дозволяє отримати максимальне значення добутку $\gamma^2\sigma_ш^2$.

Розв'язання задачі для не вироджених безперервних розподілень

Оскільки стаціонарний процес $U(t)$ — безперервний на інтервалі визначення $U \in [-U_{\max}, U_{\max}]$, задача зводиться до пошуку густини розподілення процесу $w(U)$, для якої

$$\sigma_{ш}^2 = \int_{-U_{\max}}^{U_{\max}} U^2 w(U)\, dU - \int_{-U_{\max}}^{U_{\max}} U w(U)\, dU \to \max . \tag{5}$$

Спростимо її розв'язання розглядом не вироджених на усьому інтервалі визначення симетричних відносно осі ординат густин розподілення процесу $w(U) = w(-U)$, для яких (5) спрощується:

$$\sigma_{ш}^2 = \int_{-U_{\max}}^{U_{\max}} U^2 w(U)\, dU \to \max . \tag{6}$$

Якщо ГШ генерує БГШ, обмежений знизу рівнем $-U_{\max}$ і зверху — рівнем $U_{\max}$, густину ймовірності можна подати усіченим гаусівським законом [6]:

$$w(U) = \frac{1}{\Phi\left(\frac{U_{\max}}{\sqrt{2}\sigma}\right)\sigma\sqrt{2\pi}} \exp\left[-\frac{U^2}{2\sigma^2}\right],\ U \in [-U_{\max}, U_{\max}], \tag{7}$$

де $\Phi(x)$ — функція Крампа; σ^2 — дисперсія гаусівського процесу у вільному просторі.

Дисперсія густини (7) сягає максимуму

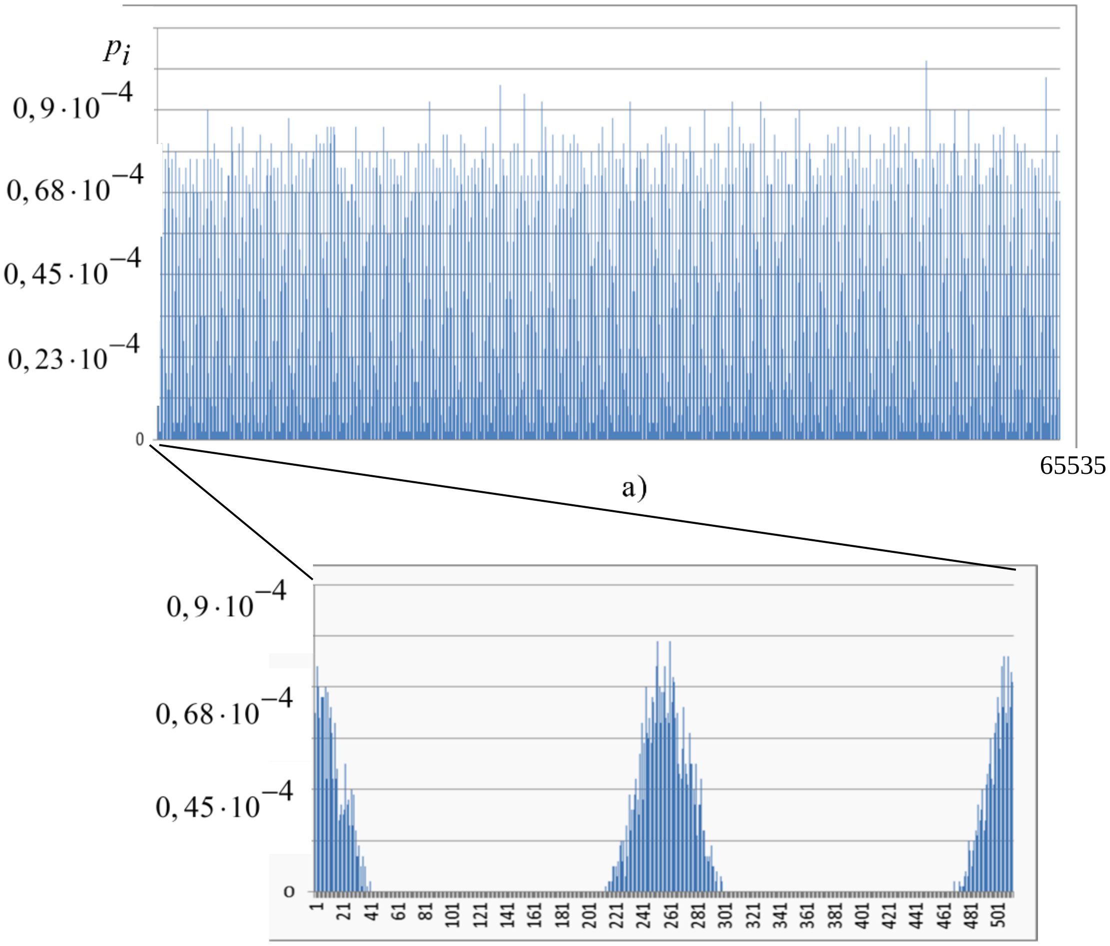
$$\sigma_{ш}^2 = \frac{U_{\max}^2}{3}, \tag{8}$$

коли $\sigma >> U_{\max}$, а сама густина ймовірності перетворюється на рівномірно розподілену:

$$w(U) = \frac{1}{2U_{\max}}\left(1 - 0\left(\frac{U^2}{\sigma^2}\right)\right),\ U \in [-U_{\max}, U_{\max}]. \tag{9}$$

Саме рівномірно, а не гаусівько-розподіленими є амплітуди, наприклад, сучасного віброакустичного ГШ «МАРС-ТЗО-4-2». Сигнал генератора був досліджений дискретизацією у 16-розрядному аналого-цифровому перетворювачі 440992 відліків шуму з подальшим розрахунком у програмному середовищі Excel розподілень амплітуд p_i. Результати обробки доводять, що розподілення p_i, $i = 0,1,..,65535$, ГШ «Марс» має рівномірний регулярний характер (див. рис. 4,*а*), а кількість амплітудних гребенів між амплітудами від 0 до 65535 сягає 256. Якщо збільшити масштаб кожного гребеня можна побачити, що його амплітуди монотонно зростають, а потім — згасають (див. рис. 4,*б*).

Таке розподілення амплітуд на виході ГШ «Марс» свідчить про те, що його МПС для формування цифрового коду шумового сигналу є 33-розрядним регістром зі зворотнім зв'язком [7], рівномірно розподілений код якого перетворюється в M = 8-розрядному ЦАП (256 градацій амплітуди) у напругу. Те, що гребінці амп-літуд (рис. 4,*б*) мають покатий характер свідчить про те, що на виході ЦАП також, як і у ГШ рис. 1, встановлений ФНЧ.



б)

Рис. 4. Оцінки розподілень амплітуд ГШ «Марс»: а) усі амплітуди; б) збільшена за масштабом частка амплітуд

Оскільки шукана густина ймовірності розподілення амплітуди ГШ $w(U)$ з максимальною дисперсією близька до рівномірно розподіленої (9), подамо її рядом:

$$w(U) = \frac{1}{2U_{\max}} \sum_{n=0}^{\infty} C_n P_n \left(\frac{U}{U_{\max}} \right), \; U \in [-U_{\max}, U_{\max}], \tag{10}$$

де $P_n(U)$ — поліноми Лежандра 1-го роду, що отримані на інтервалі ортогональності $[-U_{\max}, U_{\max}]$ з ваговою функцією $1/2U_{\max}$; C_n — деякі невідомі коефіцієнти.

Поліноми $P_n(U)$ є непарними функціями для будь-яких непарних *n*, і парними — для будь-яких парних *n*, а в силу того, що $w(U) = w(-U)$ в (10):

$$C_{2n+1} = 0, \forall n \geq 0,$$

і підстановка (10) у (6) та інтегрування в (6) призводить до необхідності виконання умови:

$$\sum_{n=0}^{\infty} \frac{C_{2n}}{\Gamma\left(\frac{5}{2}+n\right)\Gamma(2-n)} \to \max, \qquad (11)$$

де $\Gamma(x)$ — гама-функція.

Для $n \geq 2$ усі члени ряду (11) дорівнюють нулю, якщо $\forall C_{2n} \neq \infty$, а умова пошуку максимальної дисперсії спрощується:

$$\frac{C_0}{\Gamma\left(\frac{5}{2}\right)} + \frac{C_2}{\Gamma\left(\frac{7}{2}\right)} \to \max, \qquad (12)$$

і в простішому випадку, коли $C_n = 0$ для $n = 1$ та $n \geq 3$, шукана густина ймовірності (10) дорівнюватиме

$$w(U) = \frac{1}{2U_{\max}}\left(C_0 + C_2\frac{3}{2}\left(\frac{U}{U_{\max}}\right)^2 - \frac{C_2}{2}\right), \ U \in [-U_{\max}, U_{\max}], \qquad (13)$$

звідки в силу нормування: $C_0 = 1$, а в силу (12) і позитивності (13) — $C_2 = 2$. Отже, шукана густина ймовірності (13) з максимальною дисперсією

$$\sigma_ш^2 = \frac{3U_{\max}^2}{5} \qquad (14)$$

матиме параболічну густину ймовірності:

$$w(U) = \frac{3}{2U_{\max}^3}U^2, \ U \in [-U_{\max}, U_{\max}]. \qquad (15)$$

Як бачимо, (14) при тій же $U_{\max}$ майже в два рази більша за (8).

Густину ймовірності розподілення (15) можна замінити на схожу і отриману перетворенням рівномірно розподіленої фази сигналу φ, $\varphi \in [0, 2\pi]$, для гармоніки з амплітудою $U_{\max}$: $U = U_{\max} \sin(\varphi)$, для якої:

$$w(U) = \frac{1}{\pi U_{\max} \sqrt{1 - \left(\frac{U}{U_{\max}} \right)^2}}, \; U \in [-U_{\max}, U_{\max}],$$

а дисперсія — є лише на одну десяту меншою за (14):

$$\sigma_ш^2 = \frac{U_{\max}^2}{2}. \quad (16)$$

Густини ймовірностей найбільш ефективних розподілень амплітуд ГШ подано на рис. 5, з відповідними значеннями дисперсій, поданими (8), (14) та (16): суцільною лінією — для параболічного розподілення амплітуди, пунктирною — для амплітуди гармоніки з рівномірно розподіленою випадковою фазою, штрих-пунктирною — для рівномірно розподіленої амплітуди.

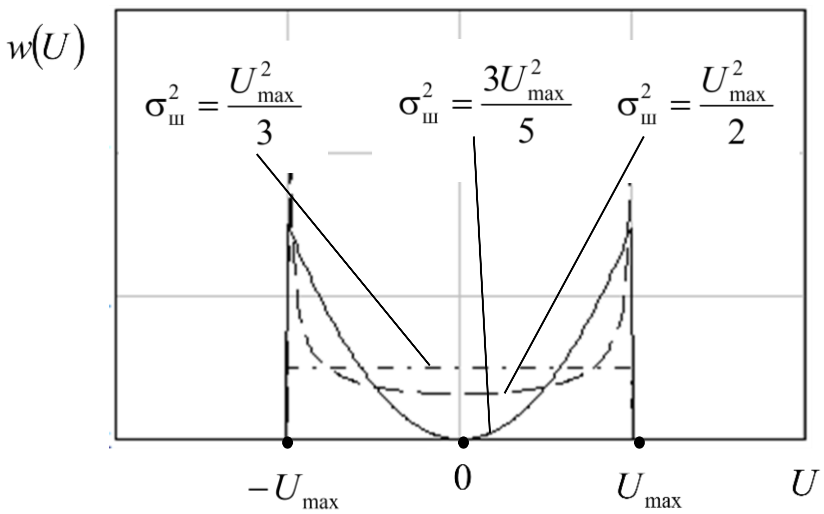


Рис. 5. Густини ймовірностей розподілень амплітуд найбільш ефективних шумових сигналів

Розв'язання задачі для дискретних кодів шумового генератора

Генерування коду i, $i = 1, \ldots, 2^M$ M-розрядного ЦАП для ГШ (див. рис. 1) з кращою ефективністю придушення ПЕМВІН, яке тим точніше відтворює (15), чим більше M матиме розподілення амплітуд:

$$p_i = \frac{3\Delta}{2U_{\max}^3} \left(-U_{\max} + i\Delta - \Delta \right)^2, \; i = 1, \ldots, 2^M, \quad (17)$$

де $\Delta = 2U_{\max} / \left(2^M - 1\right)$ — крок квантування амплітуди сигналу.

Процес генерування шуму можна спростити, якщо не наближати (16) до (15) збільшенням *M*, а навпаки покласти в генеруванні цифрових випадкових *i*-кодів схеми рис. 1: $M = 1$. При цьому на виході МПС з імовірністю p_1 генерується нуль (вихідна напруга $-U_{\max}$), та з імовірністю p_2 — одиниця (вихідна напруга $U_{\max}$), а безперервне розподілення напруги $U(t)$ на виході цифрового ГШ (див. рис. 6) є близьким до виродженого на краях інтервалу генерованих напруг:

$$w(U) = p_1\delta\left(U + U_{\max}\right) + p_2\delta\left(U - U_{\max}\right),$$

де $\delta(x)$ — дельта-функція, з дисперсією у 5/3 разів більшою за (14), яким би не були p_1 і p_2, що створюють повну групу подій.

Проте, це не означає, що структура спрощеного ГШ є кращою за подану рис. 1 з розподіленням (17). Сигнал на виході МПС рис. 6 можна вважати телеграфним [6, с. 320] з інтенсивністю пуасонівського потоку подій *λ*, спектральна густина потужності випадкового процесу якого дорівнюватиме

$$S(\omega) = \frac{2U_{\max}^2 \lambda}{\omega^2 + 4\lambda^2},$$

і нічого спільного не матиме з рівномірно розподіленим спектром частот від $2\pi F_{\min}$ до $2\pi F_{\max}$, якою би великою не була *λ*. Отже, генерування шумового сигналу за допомогою ГШ (рис. 6) є недоцільним, оскільки якість шуму залишає-ться низькою із-за нерівномірності її спектральної густини потужності.

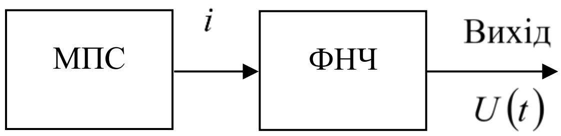


Рис. 6. Структура спрощеного ГШ для боротьби з ПЕМВІН

Висновки

1. Усічений у межах від $-U_{\max}$ до $U_{\max}$ БГШ не є кращим для активного захисту інформації від витоку через ПЕМВІН з екранів моніторів на рідинно-кристалічних структурах.

2. Для активного захисту інформації від витоку через ПЕМВІН з екранів моніторів на рідинно-кристалічних структурах кращими шумовими сигналами $U(t)$, $U(t) \in \left[-U_{\max}, U_{\max}\right]$ є сигнали, які мають максимальну дисперсією при фіксованому $U_{\max}$.

3. Кращим шумом для активного захисту інформації від витоку через ПЕМВІН з екранів моніторів на рідинно-кристалічних структурах є шум з параболічним розподіленням амплітуди.

4. У разі ускладнення розрахункової задачі під час генерування шуму з параболічним розподіленням амплітуди його можна замінити на гармоніку $U = U_{\max} \sin(\varphi)$ з рівномірно розподіленою фазою φ, $\varphi \in [0, 2\pi]$, або на рівномірно розподілену на інтервалі $[-U_{\max}, U_{\max}]$ випадкову величину.

1. Some Measurements on DVB-T Dongles with E4000 and R820 Tuners: Image Rejection, Intermodulation. URL: http://f6fvy.free.fr/rtl_sdr/Some_Measurements_on_E4000_and_R820_Tuners.pdf (Дата звернення: 04.09.2021).

2. Владимиров В.И., Владимиров И.В., Наметкин В.В. Избранные вопросы радиоэлектронного подавления цифровых сигналов систем радиосвязи. Воронеж, ВАИУ, 2010. 119 с.

3. Тетерич Н.М. Генераторы шума и измерение шумовых характеристик. Москва: Энергия, 1968. 343 с.

4. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. Москва: КУДИЦ-ОБРАЗ, 2003. 124 с.

5. Євграфов Д.В. Фізичні основи захисту інформації в радіоелектронній апаратурі: навч. посіб. Київ: НТУУ «КПІ», 2014. 176 с.

6. Левин Б.Р. Теоретические основы статистической радиотехники. Москва: Радио и связь, 1989. – 656 с.

7. Генератор віброакустичного зашумлення МАРС-ТЗО-4-2. URL: https://radio-security.com.ua/ua/p44207270-generator-vibroakusticheskogo-zashumleniya.html (Дата звернення: 04.09.2021).

Надійшла до редакції 13.10.2022