УДК 621.391

О.С. Суховерх[1], Є.М. Прокопенко[2]

[1] *Національний університет оборони України імені Івана Черняховського, Київ*
[2] *Військовий інститут телекомунікацій та інформатизації, Київ*

МАТЕМАТИЧНА МОДЕЛЬ ПРОЦЕСУ ВИЯВЛЕННЯ ТА ПОДАВЛЕННЯ НЕБЕЗПЕЧНИХ СИГНАЛІВ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

В даній статті описана математична модель процесу виявлення та подавлення небезпечних сигналів на об'єкті інформаційної діяльності. Приведені основні математичні співвідношення для обчислення ймовірностей виявлення та подавлення небезпечних сигналів. Розглянуту модель доцільно використовувати при проектуванні систем захисту інформації з пасивним випромінюванням.

Ключові слова: *технічний захист інформації, небезпечні інформаційні сигнали, завада.*

Вступ

Постановка проблеми. На сьогодні технічний захист інформації (ТЗІ) відіграє важливу роль в безпеці держави.

Значну роль в ТЗІ відіграє захист інформації від несанкціонованого доступу в об'єктах інформаційної діяльності (ОІД). Одним з напрямів по недопущенню витоку інформації є своєчасне виявлення і подавлення небезпечних інформаційних сигналів. В якості небезпечних інформаційних сигналів можуть виступати: поля, сигнали та ін. джерела, що випромінють на ОІД, як в штатному, так і в нештатному режимі функціонування, а також пристрої несанкціонованого зйому і передачі інформації.

Аналіз останніх досліджень та публікацій. В області проектування і створення комплексів із виявлення і подавлення небезпечних інформаційних сигналів накопичений значний досвід [1], але безперервне вдосконалення елементної бази, призвело до появи нових підходів до обробки і перехвату інформації на об'єктах інформаційної діяльності.

Тому ***метою статті*** є розробка математичної моделі процесу виявлення небезпечних сигналів на об'єктах інформаційної діяльності та процесу їх подавлення. Аналіз сигналів відбувається радіочастотному діапазоні.

Виклад основного матеріалу дослідження

Проведемо аналіз процесу виявлення небезпечних інформаційних сигналів, що випромінює ОІД в контрольованій зоні №1, та алгоритм функціонування засобів перехвату та подавлення сигналів (рис. 1). ОІД складається із автоматизованих робочих місць, мережевого комутатора, пристрою шифрування IP - трафіку та маршрутизатора. Засоби захисту ОІД складаються із скануючого приймача, програмно-апаратного комплексу керування та засобів подавлення небезпечних сигналів.

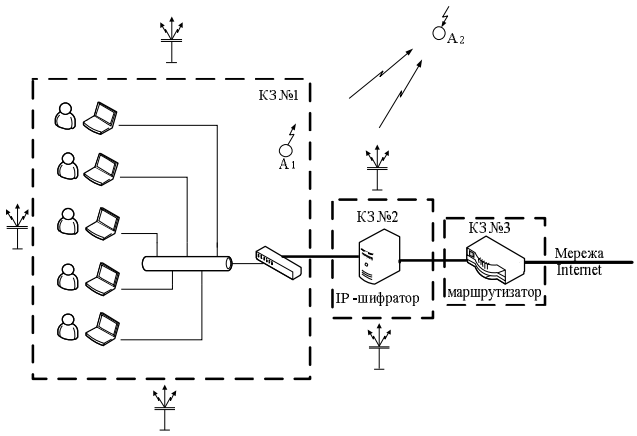

Рис. 1. Схема функціонування об'єкта інформаційної діяльності

Приймач із складу системи безперервного пошуку забезпечує виявлення небезпечних сигналів, їх селекцію та класифікацію. Оцінка сигналів проводиться на підставі відомих параметрів ОІД та можливостей зловмисника із перехвату та обробки інформації.

Розглянемо набір небезпечних інформаційних сигналів s (t), що діють в контролює мій зоні (КЗ) №1 на ОІД.

Набір небезпечних інформаційних сигналів генерується, як безпосередньо ОІД так і засобами несанкціонованого зйому і передачі інформації, що перебувають випадково чи встановлені стаціонарно, основним завданням яких є збір і передача інформації про ОІД.

Нехай за час T в просторі реєструється n реалізацій сигналу

$$s_n(t),\ t \in [(n-1)T_S, nT_S],\ n = \overline{1, N},\ T = T_S N. \quad (1)$$

На приймальному боці, зловмисник, при відсутності навмисних завад має реалізацію випадкового процесу

$$s(t) = s_n(t) + \xi(t),\ t \in [(n-1)T_S, nT_S],\ n = \overline{1, N}, \quad (2)$$

де $\xi(t)$ – адитивний гаусівський шум (рис. 2, а).

Приймач зловмисника проводить оцінку реалізації процесу $x_n(t)$ і видає рішення у вигляді сигналу $\hat{s}_n^*(t)$. На підставі аналізу і оцінки реалізацій цього сигналу проводиться аналіз і рішення щодо функціонування ОІД.

Розглянемо процес пошуку і подавлення небезпечних сигналів $s_n(t)$ засобами захисту. Приймач пошуку і виявлення небезпечних сигналів зазвичай розташований безпосередньо біля ОІД, і тому перебуває в значно кращих умовах, ніж приймач зловмисника. В лінії із виявлення небезпечних сигналів на сигнал $s_n(t)$ діє адитивна завада $\xi_1(t)$, і тому реалізація $y_n(t)$ має вигляд [2]:

$$y_n(t) = s_n(t) + o_1(t),\ t \in [(n-1)T_S, nT_S],\ n = \overline{1, N}. \quad (3)$$

У загальному випадку, приймач пошуку і виявлення небезпечних сигналів може функціонувати за алгоритмами сумісного виявлення і оцінювання сигналів, або за алгоритмами послідовного аналізу [3].

Структура навмисних завад, що генерують засоби захисту, може бути найрізноманітнішою. Прикладами типових завад і методи їх генерації приведені в [4]. Ефективним методом постановки навмисних завад є генерація завад у вигляді гармонійного коливання, що модулюється за амплітудою і фазою випадковим гаусівським процесом, зі спектральною щільністю $G_n(f)$. Навмисна завада $\eta(t)$ (рис. 2, б) може бути записана:

$$\eta(t) = V(t)\cos(\omega S\, t + \psi(t)),\quad t \in [0, T_S], \quad (4)$$

де ωS – несуча частота передачі сигналу $s_n(t)$, $\omega S = 2\pi F_S$; $V(t)$ – амплітуда навмисної завади; $\psi(t)$ – фаза навмисної завади.

Навмисна завада $\eta(t)$, яка генеруються засобами захисту, додається до випадкового процесу $x_n(t)$. Оскільки несуча частота передачі F_S сигналів $s_n(t)$ невідома, навмисна завада в точці прийому з'явиться із затримкою $\tau_B > 0$, відносно початку передачі сигналів $s_n(t)$. приймач станції пошуку небезпечних сигналів проводить безперервний пошук за заданим алгоритмом. Після виявлення факту передачі сигналів $s_n(t)$ здійснюється подавлення небезпечних сигналів навмисною завадою $\eta(t)$.

Введемо індикаторну функцію $\gamma(t \mid \tau_B)$,

$$\gamma(t \mid \tau_B) = \begin{cases} 0, \text{при } 0 \le t \le \tau_B; \\ 1, \text{при } \tau_B < t < \infty. \end{cases} \quad (5)$$

За початок передачі сигналів $s_n(t)$ встановимо час $t_0 \ge 0$, тоді реалізацію сигналу $x_n(t)$ на вході приймача зловмисника можна записати:

$$x_n(t) = s_n(t) + o(t) + \gamma(t \mid \tau_B)\eta(t);$$
$$t \in [t_0 + (n-1)T_s, t_0 + nT_s],\ n = \overline{1, N} \quad (6)$$

де $\tau_B \in [0, T]$ – представляє собою час затримки між початком випромінювання сигналу і часом, необхідним для постановки навмисних завад [3].

Якщо пошук і виявлення факту передачі небезпечних сигналів із реалізацією $y_n(t)$, відбувається у дискретні проміжки часу $T_A > 0$, то $\tau_B = kT_A$, де $k = 1, \ldots, N$ – дискретна випадкова величина [3]. Час аналізу T_A на кожному кроці пошуку має бути $T_A > 0$. Для зручності аналізу припустимо, що $T_A = T_s$, тоді за T – час передачі небезпечних сигналів, приймач пошуку зможе зробити k кроків із виявлення сигналів $s_n(t)$

$$k = \frac{T}{T_A}. \quad (7)$$

Для кількісного аналізу параметрів пошуку небезпечних сигналів необхідно знати розподіл випадкової величини τ_B, математичне очікування та дисперсію.

Припустимо, що є апріорно відома смуга частот, в якій здійснюється передача небезпечних сигналів $F_{ОІД} = F_B - F_H$ – ширина смуги частот приймача зловмисника, F_B – верхнє значення смуги частот, F_H – нижнє значення смуги частот. Для пошуку і виявлення сигналів $s_n(t)$ приймачу пошуку небезпечних сигналів необхідно проаналізувати m частот $F_A \in [F_B - F_H]$, де

$$F_A = F_H + k\Delta F,\quad k \in [\overline{1, m}],\quad m = \frac{F_B - F_H}{F_A}. \quad (8)$$

Дискретну множину частот F_A, де відбувається пошук сигналів $s_n(t)$, визначимо через $\Omega = \{F_i\}_{i=m}$ [4]. Зробимо також припущення, що $F_A \approx F_S$. Для виявлення сигналів $s_n(t)$ використовують наступні алгоритми пошуку: циклічний одноканальний із послідовним аналізом; багатоканальний з одночасним аналізом всіх m частот $F_i \in \Omega$; паралельно-послідовний пошук та ін. [4, 5].

Пошук і виявлення сигналів здійснюється за скінчену кількість кроків $k \in [1, N]$, або за скінчений час передачі T.

Генерація навмисної завади із затримкою $\tau_B \ge T$ призводить до появи завади після передачі сигналів $s_n(t)$ і подавлення не відбувається.

Для спрощення розрахунків припустимо, що $t_0 = 0$. В цьому випадку реалізація сигналу на вході приймача зловмисника можна представити (рис. 2, в):

$$x_n(t) = s_n(t) + o(t) + \gamma(t \mid \tau_B)\eta(t);$$
$$t \in [(n-1)T_s, nT_s];\ \tau_B = kT_S;\ k \in \{1, \ldots, N\},\ n = \overline{1, N},\ N = T/T_S. \quad (9)$$

Величина $o(t)$ є стаціонарним випадковим процесом з нульовим значенням математичного очікування і кінцевою дисперсією:

$$Mo(t) = 0,\quad Do(t) = y^2 > 0, \quad (10)$$

де M – оператор математичного сподівання [4]; D – оператор дисперсії; σ – середнєквадратичне відхилення випадкової величини.

На рис. 2, г показаний процес $з(t)$ появи навмисної завади із нульовим значенням математичного сподівання і кінцевою дисперсією:

$$Mз(t) = 0, \quad Dз(t) = y_з^{\,2} \geq 0, \qquad (11)$$

де $y_з^{\,2}$ – дисперсія навмисної завади в точці A_2.

Введемо суми завад, що приходять в точку прийому A_2:

$$o(t \mid \tau_B) = o(t) + г(t \mid \tau_B) з(t), \quad t \in [t_0, t_0 + T]. \qquad (12)$$

Дисперсія:

$$y^2(t \mid \tau_B) = Do(t \mid \tau_B), \; t \in [t_0, t_0 + T], \; \tau_B \geq 0. \qquad (13)$$

Оскільки процеси $o(t)$, $з(t)$ статистично незалежні, то дисперсія $y^2(t \mid \tau_B)$ може бути записана:

$$y^2(t \mid \gamma_B) = y_o^2 + \gamma(t \mid \tau_B) y_з^2, \; t, \tau_B \in [t_0, t_0 + T]. \qquad (14)$$

Відношення сигнал-шум у випадку дії тільки однієї завади $\xi(t)$ [6]:

$$q_0^2 = E_S / G_0 = h^2 F_S T_S, \; h^2 = P_S / \sigma_0^2, \qquad (15)$$

де $P_S = E_S / T_S$ – середня потужність сигналу; G_0 [Вт/Гц] – рівномірна спектральна щільність.

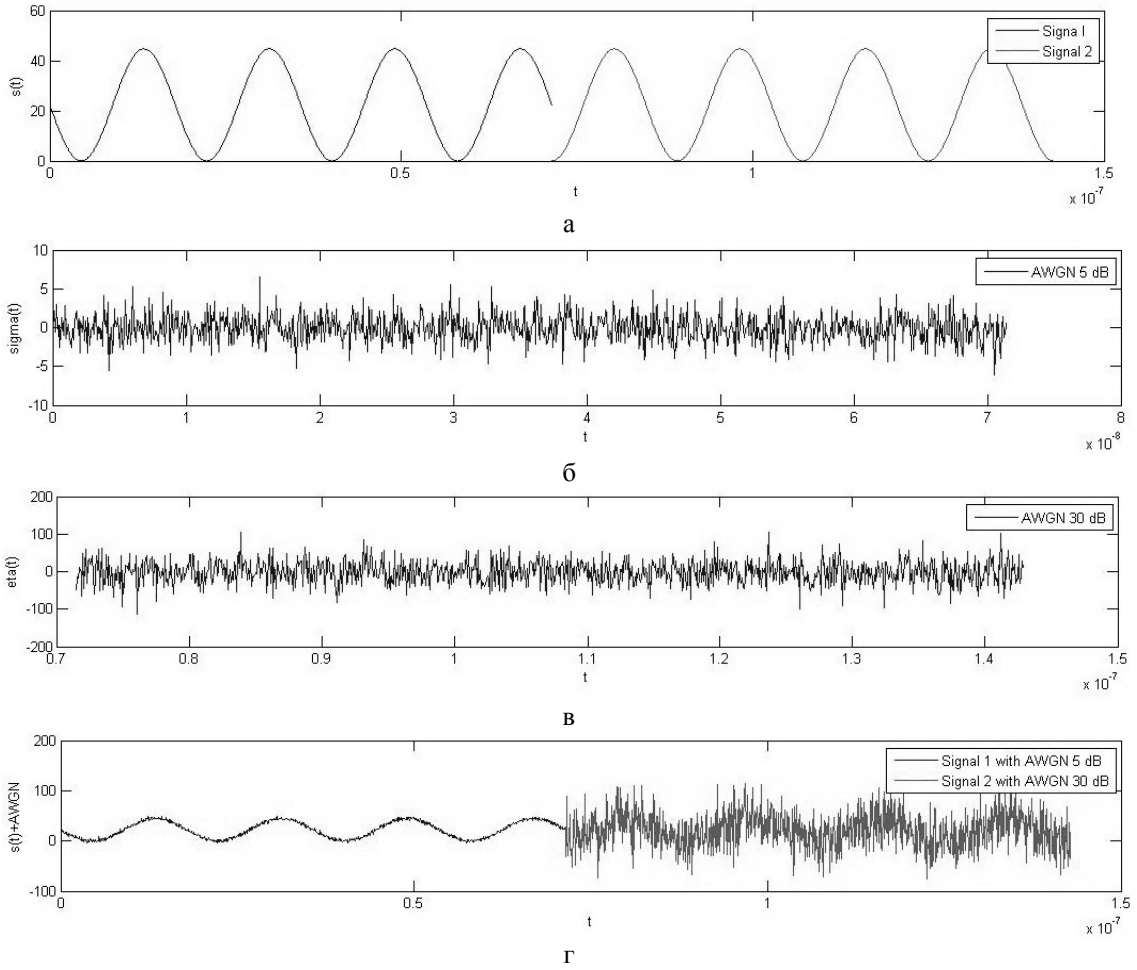

Рис. 2. Діаграма впливу навмисних завад

Припустимо, що лінійний тракт передавача небезпечних сигналів має ідеальну прямокутну характеристику із загальною шириною смуги $F = 2\,\Delta F_S$.

Нехай навмисна завада $з(t)$ має рівномірну спектральну щільність $G_З$ [Вт/Гц], тоді відношення сигнал-шум

$$q_1^2 = \frac{E_S}{G_0 + G_З} = \frac{E_S}{G_1} = h_1^2 F_S T_S, \; h_1^2 = \overline{y_1^2}, \qquad (16)$$

де $G_1 = G_0 + G_З$ – спектральна щільність суми завад $o_1(t) = o(t) + з(t)$; y_1^2 – дисперсія суми завад.

Введемо відношення сигнал-шум:

$$q^2(t \mid \tau_B) = \begin{cases} q_0^2, \text{при } t_0 \leq t \leq t_0 + \tau_B, \\ q_1^2, \text{при } t_0 + \tau_B \leq t \leq T. \end{cases} \qquad (17)$$

Відомо [5, 6], що практично в будь-якій схемі прийому сигналів ймовірність помилки є поступово зменшувальною функцією від величини відношення сигнал-шум.

При зменшенні відношення сигнал-шум, ймовірність помилки сигналу збільшується, $q_0 > q_1$, $P_S(q_0) < P_S(q_1)$.

В умовах дії навмисних завад при зміні $q^2(t)$ ймовірність помилки $P_S(q)$ також буде змінюватись.

Таким чином, якщо виявлення факту передачі відбувається у випадкові моменти часу $\tau_B \in [t_0, t_0 + T]$, то перші $k = \tau_B / T_S$ сигналів $s_n(t)$ приймаються на фоні гаусівського шуму $\xi(t)$, а інші $N - k$ на фоні навмисної завади

$$\xi_1(t) = \xi(t) + \eta(t).$$

Розрізнення $k \in [1, \ldots, N]$ сигналів проводиться із ймовірністю $P_{S_0} = P_S(q_0)$, а розрізнення решти $N - k$ сигналів із ймовірністю $P_{S1} = P_S(q_1)$.

Якщо зафіксувати $\tau_B = kT_S$, то отримаємо середню ймовірність помилки для всієї сукупності N сигналів $s_n(t)$, яку позначимо $P_S(N \mid k)$.

Виконавши нескладні перетворення:

$$P_S(N \mid k) = P_{S0}\frac{k}{N} + (1 - \frac{k}{N})P_{S1}, \quad k \in [1, \ldots, N]. \quad (18)$$

З цього виразу видно, що при $k = N$, $P_S(N \mid k) \to P_{S_0}$. Це означає, що на виявлення сигналів $s_n(t)$ був витрачений весь час, а прийом інформації відбувся без впливу навмисних завад. З іншого боку, якщо $k = 0$, що є ідеальним випадком для системи постановки навмисних завад, прийом інформації відбувається тільки при дії навмисних завад.

Ймовірності P_{S1} і P_{S0} визначаються:

$$P_{S0} = P_S(q_0; M);$$

$$P_{S1} = P_S(q_1; M) \equiv P_S(\frac{q_0}{H_{01}}; M); \quad (19)$$

$$q_1 < q_0, \quad P_S(q_0) < P_S(q_1),$$

де $H_{01} = q_0^2 / q_1^2$.

Збільшення ймовірності помилки до $P_S(q_1)$ призводить до неможливості прийому інформації зловмисником.

Висновки

В статті розроблена математична модель процесу виявлення та подавлення небезпечних сигналів на об'єкті інформаційної діяльності.

Наведена вище модель рекомендується для використання при проведенні розрахунків рівня захищеності на об'єктах інформаційної діяльності, коли є ризик перехоплення інформації під час обробки до того, коли вона буде зашифрована.

Напрямки подальших досліджень будуть направлені на розробку методики підвищення ефективності захисту об'єктів інформаційної діяльності при впливі небезпечних сигналів.

Список літератури

1. Обнаружение радиосигналов / [П.С. Акимов, Ф.Ф. Евстратов, С.И. Захаров и др.]; под ред. А.А. Колосова. – М.: Радио и связь, 1989. – 288 с.

2. Борисов В.И. Помехозащищенность систем радиосвязи. Вероятностно-временной подход / В.И. Борисов, В.М. Зинчук. – М.: РадиоСофт, 2008. – 260 с.

3 .Управление радиочастотным спектром и электромагнитная совместимость радиосистем [учебн. пос.] / Под ред. М.А. Быховского, – М.: Эко-Трендз, 2006. – 376 с.

4. Теория обнаружения сигналов / [П.С. Акимов, П.А. Бакута, В.А. Богданович и др.]; под ред. П.А. Бакута. – М.: Радио и связь, 1984. – 440 с.

5. Журавлев В.И. Поиск и синхронизация в широкополосных системах / В.И. Журавлев – М.: Радио и связь, 1986. – 240 с.

6. Современная радиоэлектронная борьба. Вопросы методологии. / Под ред. В.Г. Радзиевский. – М.: Радиотехника, 2006 – 424 с.

Надійшла до редколегії 23.06.2016

Рецензент: д-р техн. наук, проф. О.В. Кувшинов, Військовий інститут телекомунікацій та інформатизації, Київ.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПРОЦЕССА ОБНАРУЖЕНИЯ И ПОДАВЛЕНИЯ ОПАСНЫХ СИГНАЛОВ НА ОБЪЕКТАХ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ

А.С. Суховерх, Е.Н. Прокопенко

В данной статье описана математическая модель процесса обнаружения и подавления опасных сигналов на объектах информационной деятельности. Приведены основные математические соотношения для расчета вероятностей обнаружения и подавления опасных сигналов. Рассмотренную модель целесообразно использовать при проектировании систем защиты информации с пассивным излучением.

Ключевые слова: *техническая защита информации, опасные информационные сигналы, помеха.*

MATHEMATICAL MODEL OF DETECTION AND SUPPRESSION OF DANGEROUS SIGNALS AT THE OBJECTS OF INFORMATION ACTIVITY

O.S. Sukhoverkh, Ye.M. Prokopenko

This article describes a mathematical model of detection and suppression of dangerous signals at the object of information activity. Basic mathematical equations to calculate the probability of detection and suppression of dangerous signals were examined. The model should be used in the process of designing information security systems with passive radiation.

Keywords: *technical protection of information, dangerous information signals, obstacle.*