DOI: 10.18372/2225-5036.30.19209

ОБҐРУНТУВАННЯ ВИРІШАЛЬНОЇ СХЕМИ ДЛЯ ОЦІНЮВАННЯ ІМОВІРНОСТІ ДЕТЕКТУВАННЯ ЕЛЕКТРОМАГНІТНИХ СИГНАЛІВ З МЕТОЮ УНЕМОЖЛИВЛЕННЯ ЇХ ВИЯВЛЕННЯ

Сергій Іванченко, Василь Некоз

Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського"

ІВАНЧЕНКО Сергій Олександрович, д.т.н., професор
Рік та місце народження: 1970 рік, с.м.т. Іванків Київської обл.
Освіта: Київське вище військове училище зв'язку ім. М.І. Калініна.
Посада: професор Спеціальної кафедри № 1 Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського".
Наукові інтереси: кібербезпека, захист інформації.
Публікації: більше 100 публікацій, серед яких наукові статті.
E-mail: soivanch@ukr.net.
Orcid ID: 0000-0003-1850-9596.

НЕКОЗ Василь Сергійович, викладач
Рік та місце народження: 1987 рік, м. Винники Львівської обл.
Освіта: військовий інститут телекомунікацій та інформатизації Національного технічного університету України "Київський політехнічний інститут".
Посада: Викладач Спеціальної кафедри № 3 Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського".
Наукові інтереси: кібербезпека, захист інформації.
E-mail: nvs20141987@gmail.com.
Orcid ID: 0000-0001-5091-0529.

Анотація*. Проведено обґрунтування вирішальної схеми для побудови приймача з метою здійснення можливого детектування ознак сигналів в просторі. Відповідно до умови щодо унеможливлення детектування ознак небезпечних сигналів для побудови вирішальної схеми приймача обґрунтовано критерій оптимальності. Його отримано за максимумом демаскування інформаційних сигналів, переслідуючи виконання умови захищеності, як для найгіршого випадку. Тобто, якщо не визначаються сигнали з більш демаскувальними ознаками, наприклад, потужністю, то не визначатимуться сигнали і з менш демаскувальними ознаками. На основі отриманого критерію оптимальності побудовано відповідну вирішальну схему оптимального приймача. Запропонована схема розглядає три гіпотези: ознаки сигналу відсутні, неможливість впевненого визначення ознак сигналу та ознаки сигналу присутні. На основі зазначеної вирішальної схеми отримано її приватний випадок, який описує умову неможливості впевненого виявлення ознак небезпечного сигналу в той час, коли ІКС або технічні засоби обробки та передачі інформації, працюють. Дискретно-неперервний канал із використанням зазначеної схеми дозволяє імітувати технічний канал витоку інформації, як для найгіршого випадку з точки зору захищеності, та знайти імовірність неможливості впевненого виявлення ознак небезпечного сигналу. Як очевидно, ця імовірність визначатиме імовірність ризику безпеки.*

Ключові слова: *інформаційна безпека, кібербезпека, інформаційно-комунікаційні системи, системи захисту інформації, інформаційний сигнал, дискретний канал.*

Постановка проблеми

Одним із завдань інформаційної безпеки є захист інформації щодо забезпечення її конфіденційності, цілісності та доступності, який в частині безпеки інформаційного простору передбачає захист інформації від її неконтрольованого поширення. Канали витоку є паразитним утворенням під час роботи технічних засобів та систем обробки і передачі інформації. Вони є наслідком таких ефектів як побічні випромінювання електромагнітних полів небезпечних сигналів, наведення цих полів на сторонні провідники та технічні засоби, що мають гальванічний зв'язок з навколишнім світом, просочування небезпечних сигналів у ланцюги електроживлення та заземлення тощо.

Зазначені явища можуть приводити до витоку інформації, а тому вимагають їх усунення, або доведення до безпечного стану.

Аналіз останніх досліджень та публікацій

Особливо актуальною зазначена загроза стає для конфіденційної інформації, яка у випадку інциденту може призвести до неконтрольованого її поширення [1]. Як очевидно, це є категорично недопустимим та вимагає вжиття відповідних заходів. Для цього мають місце загальноприйняті стандарти з захисту інформації, які повинні бути забезпеченими на всіх об'єктах де циркулює певна інформація. Під захищеністю інформації має місце неможливість отримання смислового змісту з небезпечних сигналів, детектованих в просторі, що досягається шляхом забезпечення відповідних характеристик, а саме - відношення сигнал/завада.

В зв'язку з розвитком науки і техніки сучасні засоби обробки та передачі інформації зазнали суттєвих змін. Так, сучасні інформаційно-комунікаційні системи (ІКС) є високошвидкісними, багатофункціональними та самокерованими системами з мінімум залучення оператора управління. Вони використовують сучасну елементну базу з високим степенем інтеграції та, відповідно, широкосмугові високочастотні сигнали, самостійно вносять в повідомлення надлишковість та керують повторами сеансів для коригування помилок. Сучасні ІКС мають швидку зміну поколінь та перспективу розвитку, що пов'язана з розширенням спектру використовуваних сигналів та з можливою зміною носія інформації. На сьогоднішній день не могла не зазнати розвитку і техніка перехоплення та обробки небезпечних сигналів. Так, аналіз доступної літератури показав, що на сьогоднішній день ефективним засобом прийому є аналізатор спектру. З їх використанням можлива реалізація майже ідеального приймача [2].

Мета та постановка завдання

Метою статті є обґрунтування побудови вирішальної схема приймача та оцінювання імовірності детектування ознак небезпечного сигналу.

Виклад основного матеріалу дослідження

Для побудови вирішальної схеми оптимального приймача щодо виявлення ознак небезпечних сигналів в каналах витоку виразимо $\lambda_{q/0}(u)$ через характеристики дискретного джерела та дискретно-неперервного каналу побудуємо вирішальну схему оптимального приймача.

Якщо інформаційний сигнал $s_q(t)$ фінітний та повністю зосереджений в спектрі частот F, то для каналу, лінійно ослаблений $c_q(t)$ та вся корисна інформація в сигналі $u(t)$ на виході каналу будуть повністю зосередженими в цьому спектрі частот. Виходячи з цього, за теоремою Котельникова шукані відношення правдоподібності можна представити в $k = 2FT$ відліках сигналу $u(t)$ [7]:

$$\lambda_{q/0}(u_1,u_2,...,u_{2FT}) = \frac{\omega(u_1,u_2,...,u_{2FT}/x_q)}{\omega(u_1,u_2,...,u_{2FT}/x_0)}. \qquad (1)$$

де $\omega(u_1,u_2,..u_{2FT}/x_q)$ – умовна $2FT$-вимірна щільність розподілу ймовірностей неперервних значень u на виході каналу, якщо на його вхід потрапив знак x_q.

Якщо на вхід приймача потрапляє суміш $u(t) = c_r(t) + n(t)$ у виді відліків $u_i = c_{ri} + n_i$, то за умови статистичної незалежності нормально розподілених $2FT$-мірна умовна щільність ймовірностей визначається за формулою:

$$\omega(u_1,u_2,...,u_{2FT}/x_r) = \omega(u_1 - c_{r1}, u_2 - c_{r2},...,u_{2FT} - c_{r2FT}/0) =$$
$$= \frac{1}{(\sigma\sqrt{2\pi})^{2FT}} \exp\left\{-\frac{1}{2\sigma^2}\sum_{i=1}^{2FT}(u_i - c_{ri})^2\right\}. \qquad (2)$$

Підставивши (2) в (1), знайдемо відношення правдоподібності для x_q за заданою вибіркою $u(t)$:

$$\lambda_{q/0}(u_1,u_2,...,u_{2FT}) = \exp\left\{\frac{1}{2\sigma^2}\sum_{i=1}^{2FT}(u_i - c_{0i})^2\right\} \cdot \exp\left\{-\frac{1}{2\sigma^2}\sum_{i=1}^{2FT}(u_i - c_{qi})^2\right\}. \qquad (3)$$

При умові, що якщо в каналі діє завада у вигляді білого шуму зі спектральною щільністю N_0, то при спрямуванні ширини спектру $F \to \infty$ відношення правдоподібності:

$$\lambda_{q/0}(u) = \lim_{F\to\infty}\left[\begin{array}{l}\exp\left\{\frac{1}{N_0}\sum_{i=1}^{2FT}(u_i - c_{0i})^2\Delta t\right\} \\ \exp\left\{-\frac{1}{N_0}\sum_{i=1}^{2FT}(u_i - c_{qi})^2\Delta t\right\}\end{array}\right] =$$
$$= \exp\left\{\frac{1}{N_0}\left[\int_0^T [u(t) - c_0(t)]^2 dt - \int_0^T [u(t) - c_q(t)]^2 dt\right]\right\} =$$
$$= \exp\left\{\begin{array}{l}\left[\frac{2}{N_0}\int_0^T u(t)c_q(t)dt - \frac{P_q T}{N_0}\right] - \\ -\left[\frac{2}{N_0}\int_0^T u(t)c_0(t)dt - \frac{P_0 T}{N_0}\right]\end{array}\right\} =$$
$$= \exp\left\{\frac{2T}{N_0}\left[Z_q(u) - \frac{P_q}{2}\right] - \left[Z_0(u) - \frac{P_0}{2}\right]\right\}, \qquad (4)$$

де P_r – потужність реалізації $c_r(t)$:

$$P_r = \frac{1}{T}\int_0^T c_r^2(t)dt, \qquad (5)$$

$z_q(u)$ та $z_0(u)$ – допоміжні величини, що мають сенс взаємної потужності підінтегральних сигналів. Для довільного r вона визначається формулою:

$$z_r(u) = \frac{1}{T}\int_0^T u(t)c_r(t)dt, \qquad (6)$$

N_0 – спектральна щільність білого шуму, який використано в якості маскувальної завади.

Зауважимо, що якщо "нульова" реалізація $c_0(t) = 0$, то співвідношення (4) дещо спроститься:

$$\lambda_{q/0'}(u) = \exp\left\{\frac{2T}{N_0}\left[Z_q(u) - \frac{P_q}{2}\right]\right\}. \quad (7)$$

Не важко також побачити, що відношення правдоподібності для "нульової" реалізації $c_0(t) \neq 0$ можна виразити з використанням (7) для $c_0(t) = 0$:

$$\lambda_{q/0}(u) = \exp\left\{\frac{2T}{N_0}\left[Z_q(u) - \frac{P_q}{2}\right] - \left[Z_0(u) - \frac{P_0}{2}\right]\right\} = \frac{\exp\left\{\frac{2T}{N_0}\left[Z_q(u) - \frac{P_q}{2}\right]\right\}}{\exp\left\{\frac{2T}{N_0}\left[Z_0(u) - \frac{P_0}{2}\right]\right\}} = \frac{\lambda_{q/0'}(u)}{\lambda_{0'/0}(u)}, \quad (8)$$

де $\lambda_{0'/0}(u)$ – відношення правдоподібності ненульової "нульової" реалізації $c_0(t) \neq 0$:

$$\lambda_{0'/0}(u) = \frac{\omega(u/x_0)}{\omega(u/0)} = \frac{\omega(u/x_0)}{\omega(n)} = \exp\left\{\frac{2T}{N_0}\left[Z_0(u) - \frac{P_0}{2}\right]\right\}. \quad (9)$$

Підставивши (8) в наступне співвідношення критерію:

$$p(x_q/u) < p(x_0/u), \quad (10)$$

отримаємо:

$$\frac{\lambda_{q/0'}(u)}{\lambda_{0'/0}(u)} < \frac{p(x_0)}{p(x_q)}, \quad (11)$$

або

$$\exp\left\{\frac{2T}{N_0}\left[Z_q(u) - \frac{P_q}{2}\right] - \left[Z_0(u) - \frac{P_0}{2}\right]\right\} < \frac{p(x_0)}{p(x_q)}. \quad (12)$$

Прологарифмувавши (12) натуральним логарифмом отримаємо:

$$\frac{2T}{N_0}\left[Z_q(u) - \frac{P_q}{2}\right] - \frac{2T}{N_0}\left[Z_0(u) - \frac{P_0}{2}\right] < \ln p(x_0) - \ln\sum_{r=1}^{n} p(x_r), \quad (13)$$

або

$$Z_q(u) - \frac{P_q}{2} + \frac{N_0}{2T}\ln p(x_q) < Z_0(u) - \frac{P_0}{2} + \frac{N_0}{2T}\ln p(x_0), \quad (14)$$

На основі (14) вирішальна схема оптимального приймача перехоплення з метою виявлення в суміші прийнятого сигналу наявності інформаційних знаків за максимум демаскуючих ознак матиме вигляд, як показано (рис. 1).

Нерівність (14), за якою побудована вирішальна схема оптимального приймача перехоплення з метою виявлення ознак сигналу за максимумом демаскування реалізацій інформаційних знаків, та сама вирішальна схема представляють собою загальний ідеалізований випадок [2].

Роботу дискретно-неперервного каналу як імітацію каналу витоку разом з отриманою схемою з виділенням умови захищеності інформації від витоку можна сформулювати наступним чином.

На виході джерела інформації (рис 2) в певному тестовому режимі формуються інформаційні знаки x_0 або x_q, яким в "модуляторі" ставляться у відповідність неперервні реалізації $s_0(t)$ та $s_q(t)$.

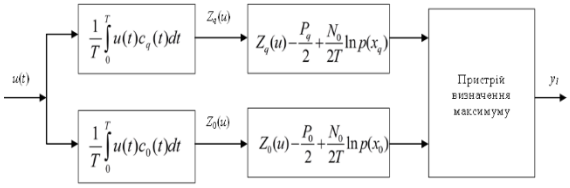

Рис. 1. Вирішальна схема оптимального приймача перехоплення з описом умови неможливості виявлення ознак сигналу за максимумом демаскування реалізацій інформаційних знаків

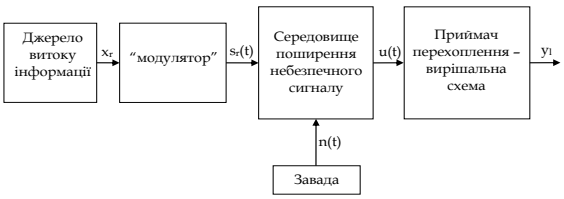

Рис. 2. Дискретно-неперервний канал як модель каналу витоку від дискретних джерел

Реалізація $s_0(t)$ означає, що ОІД, як джерело витоку не працює, тобто на виході джерела інформаційні знаки та реалізації відсутні. Слід зазначити, що так названа "нульова" реалізація $s_0(t)$ не обов'язково може дорівнювати нулю. В ряді випадків вона може бути і не "нульовою", наприклад, при використанні в ІКС фазової модуляції, або у випадку використання $s_0(t)$, як імітацію роботи ІКС з метою введення противника в оману.

Реалізація $s_q(t)$ взята із всіх реалізацій $s_r(t)$ інформаційних знаків на виході джерела, $r = 1 \div n$, n – об'єм алфавіту джерела. Реалізація $s_q(t)$ свідчить про те, що ІКС працює та обробляє інформацію. Ці реалізації поширюються в середовищі каналу витоку та надають можливість щодо прийому інформаційних сигналів, принаймні судити про те ІКС працює чи ні.

На сигнал $s_q(t)$ в середовищі поширення діє адитивна завада, нехай білий шум зі спектральною щільністю N_0. Суміш сигналу та завади поступає на вирішальну схему та приймає рішення y_l. Якщо, приймач визначив, що $l = q$, то це означає, що ІКС працює та обробляє інформацію. Якщо ж $l = 0$, то це означає, що ІКС не працює, інформація не обробляється.

Імовірності $p(x_0)$ та $p(x_q)$ є апріорними імовірностями того, що ІКС, відповідно, не працює – на виході джерела має місце реалізація $s_0(t)$ або ІКС працює – на виході джерела має місце узагальнена реалізація $s_q(t)$.

Однак, як відомо будь-який вимірювальний приймач або пристрій не може здійснювати абсолютно точні вимірювання. Як правило, кожен з них має свій поріг чутливості або похибку. Чутливість радіоприймача характеризується його здатністю забезпечувати прийом корисного радіосигналу на фоні власних шумів при відсутності радіозавад і відтворювати його на виході із заданою якістю. Кількісно цей параметр визначається мінімально необхідною потуж-

ністю сигналу в антені, при якій забезпечується номінальне значення напруги або потужності на виході приймача, при заданих параметрах модуляції радіосигналу й відношенні сигнал/шум на виході.

Так, якщо існує порогове, яке відображає чутливість приймача, позначимо його як нульова порогова реалізація $c_{0\,\text{пор.}}(t)$, то нерівність (14) можна переписати у виді:

$$Z_q(u) - \frac{P_q}{2} + \frac{N_0}{2T}\ln p(x_q) < \\ < \max\begin{bmatrix} Z_{0\,\text{пор.}}(u) - \dfrac{P_{0\,\text{пор.}}}{2} + \dfrac{N_0}{2T}\ln p(x_q); \\ Z_{0\,\text{пор.}}(u) - \dfrac{P_{0\,\text{пор.}}}{2} + \dfrac{N_0}{2T}\ln p(x_0) \end{bmatrix} < \\ < Z_0(u) - \frac{P_0}{2} + \frac{N_0}{2T}\ln p(x_0), \qquad (15)$$

де $P_{0\ \text{пор.}}$ – порогова потужність сигналу $c_{0\,\text{пор.}}(t)$:

$$P_{0\ \text{пор.}} = \frac{1}{T}\int_0^T c^2_{0\ \text{пор.}}(t)dt, \qquad (16)$$

$Z_{0\,\text{пор.}}(u)$ – взаємна потужність сигналів $u(t)$ та порогового $c_{0\,\text{пор.}}(t)$:

$$Z_{0\ \text{пор.}}(u) = \frac{1}{T}\int_0^T u(t)c_{0\text{пор.}}(t)dt. \qquad (17)$$

Як очевидно, нерівність (15) на відміну нерівності (14) характеризує стан вирішальної схеми приймача не як одну із двох гіпотез, а як одну з трьох:

– неможливість виявлення ознак інформаційного сигналу;

– неможливість впевненого виявлення ознак інформаційного сигналу;

– виявлення ознак небезпечного сигналу.

Крім того очевидно, що нерівність (15) залежить ще й від розподілу апріорних імовірностей $p(x_0)$ та $p(x_q)$. Не складно помітити, що при фіксованому $c(t)$ не залежно від його рівня, при $p(x_0) > p(x_q)$ гіпотеза невиявлення ознак небезпечного сигналу проявлятиметься частіше ніж при $p(x_q) > p(x_0)$.

Зазначене зручно представити у виді шкали на рис. 3, яка побудована для випадку рівності імовірностей $p(x_0) = p(x_q)$ (рис. 3).

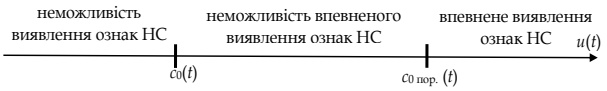

Рис. 3. Шкала стану приймача щодо неможливості виявлення ознак на осі рівня небезпечного сигналу з відмітками нулової реалізації та чутливості вимірювального приймача

Відповідно до нерівності (15) вирішальну схему приймача можна представити у виді як показано (рис. 4).

Якщо в нерівності (15) ліва частина приймає максимум, то це означає, що приймач фіксує ознаки небезпечного сигналу $c_q(t)$, який характеризується максимальними демаскуючими ознаками. Якщо ж нерівність виконується, тобто максимуму досягають сердня, або ліввa частини, то вирішальна схема приймає рішення не про неможливість впевненого виявлення або відсутність ознак небезпечного сигналу в середовищі його поширення. За умови надходження до приймача сигналів з рівнем менше порогового, завдяки власним шумам, цей приймач знаходиться у стані повної невизначеності.

Цей стан приймача називатимемо неможливістю його щодо впевненого виявлення ознак небезпечного сигналу. За цього стану приймач реально "не бачить" на вході ніяких сигналів, а "бачить" лише власні шуми. Вище сказане зручно зобразити за допомогою залежності станів приймача від значення корисного сигналу, що потрапляє на його вхід.

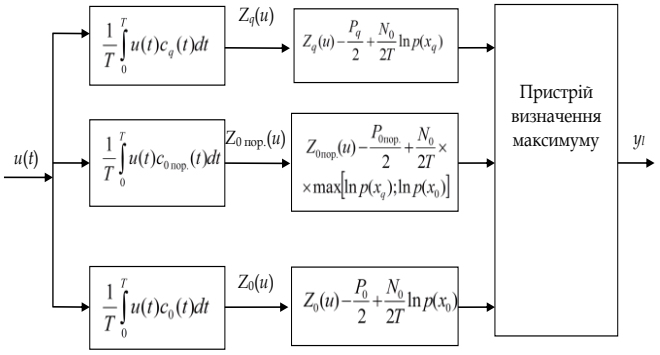

Рис. 4. Вирішальна схема оптимального приймача з описом умови неможливості виявлення та впевненого виявлення ознак інформаційного сигналу за максимумом демаскування реалізацій інформаційних знаків з врахуванням порогу чутливості приймача

Цей стан приймача називатимемо неможливістю його щодо впевненого виявлення ознак небезпечного сигналу. За цього стану приймач реально "не бачить" на вході ніяких сигналів, а "бачить" лише власні шуми. Вище сказане зручно зобразити за допомогою залежності станів приймача від значення корисного сигналу, що потрапляє на його вхід. Як очевидно, умова неможливості впевненого виявлення приймачем ознак інформаційного сигналу, тобто умова, за якої приймач "не бачить" сигналу, може гарантувати й відсутність інформації в ТКВ. Немає сигналу – немає й інформації.

Оскільки, з точки зору захищеності інформації від витоку нас цікавить коли ІКС працює, а зловмисник не може виявити чи впевненого виявлення ознак небезпечного сигналу, то нерівність (15) та вирішальну схему на рис. 3 можна дослідити за умови, що $p(x_0) = 0$ та $p(x_q) = 1$.

По суті це є найгіршою умовою з точки зору захищеності, оскільки збільшення $p(x_0)$ та зменшення $p(x_q)$ приводитиме до зменшення шансів зловмисника перехоплювати інформацію. Якщо для найгіршого випадку джерело витоку буде захищеним, то за умови його покращення захищеність забезпечуватиметься із запасом. Проведемо аналіз нерівностості (14) перетворимо його, підставивши числові значення імовірностей $p(x_0) = 0$, $p(x_q) = 1$ та прирівнявши нульову реалізацію до нуля $c_0(t) = 0$. В результаті отримаємо:

$$Z_q(u) - \frac{P_q}{2} + 0 < \max\begin{bmatrix} Z_{0\ \text{пор.}}(u) - \dfrac{P_{0\ \text{пор.}}}{2} + 0; \\ Z_{0\ \text{пор.}}(u) - \dfrac{P_{0\ \text{пор.}}}{2} - \infty \end{bmatrix} < -\infty. \qquad (18)$$

Так, якщо існує порогове $c_{\text{пор.}}(t)$, яке відображає чутливість приймача, то нерівність (14) можна переписати у виді:

$$Z_q(u) - \frac{P_q}{2} < Z_{0\ \text{пор.}}(u) - \frac{P_{0\ \text{пор.}}}{2}. \quad (19)$$

За нерівністю (18) схема вирішальної схеми прийме вид як показано (рис. 5).

Схему на рис. 5 можна спростити, перетворивши нерівність (19) в дещо інший вид. Для цього перенесемо випадкові складові в ліву частину, а інші в праву. Отримаємо:

$$Z_q(u) - Z_{0\ \text{пор.}}(u) < \frac{P_q - P_{0\ \text{пор.}}}{2}. \quad (20)$$

Підставивши у (3) співвідношення для взаємної потужності $Z_{0\ \text{пор.}}(u)$ (6) та перетворивши отримаємо:

$$\frac{1}{T}\int_0^T u(t)(c_q(t) - c_{0\ \text{пор.}}(t))dt < \frac{P_q - P_{0\ \text{пор.}}}{2}, \quad (21)$$

$$\frac{1}{T}\int_0^T u(t)c_{\Delta\ \text{пор.}}(t)dt < \frac{P_q - P_{0\ \text{пор.}}}{2}. \quad (22)$$

Схему на рис. 5 можна спростити, перетворивши нерівність 19 в дещо інший вид. Для цього перенесемо випадкові складові в ліву частину, а інші в праву. Отримаємо:

$$Z_q(u) - Z_{0\ \text{пор.}}(u) < \frac{P_q - P_{\text{о пор.}}}{2}. \quad (23)$$

Підставивши у (19) співвідношення для взаємної потужності $Z_{0\ \text{пор.}}(u)$ (6) та (17) та перетворивши отримаємо:

$$\frac{1}{T}\int_0^T u(t)(c_q(t) - c_{0\ \text{пор.}}(t))dt < \frac{P_q - P_{0\ \text{пор.}}}{2}. \quad (24)$$

Виразимо потужності та вхідний сигнал до вирішальної схеми через їх формули:

$$\frac{1}{T}\int_0^T (c_q(t) + n(t))(c_q(t) - c_{0\ \text{пор.}}(t))dt < \\ < \frac{1}{2T}\int_0^T c_q^2(t)dt - \frac{1}{2T}\int_0^T c_{0\ \text{пор.}}^2(t)dt \quad (25)$$

Розкриємо дужки в лівій частині нерівності та перенесемо з лівої в праву всі доданки, що не містять випадкових величин:

$$\frac{1}{T}\int_0^T n(t)c_{\Delta\ \text{пор.}}(t)dt < \\ < -\frac{1}{2T}\int_0^T c_q^2(t)dt + 2\frac{1}{2T}\int_0^T c_q(t)c_{0\ \text{пор.}}(t)dt - \\ -\frac{1}{2T}\int_0^T c_{0\ \text{пор.}}^2(t)dt, \quad (26)$$

де $c_{\Delta\ \text{пор.}}$ – різницевий сигнал відносно порогового сигналу:

$$c_{\Delta\ \text{пор.}}(t) = c_q(t) - c_{0\ \text{пор.}}(t). \quad (27)$$

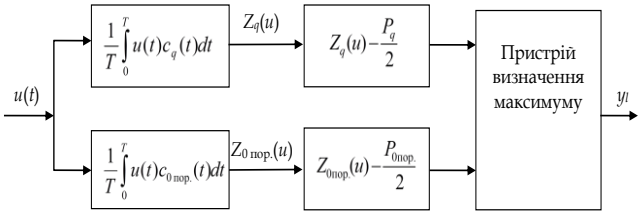

Рис. 5. Вирішальна схема оптимального приймача перехоплення з описом умови неможливості впевненого виявлення ознак небезпечного сигналу за максимумом демаскування реалізацій інформаційних знаків

Звернемо увагу, що в правій частині нерівності має місце розкладений квадрат різниці. Зведемо його:

$$\frac{1}{T}\int_0^T n(t)c_{\Delta\ \text{пор.}}(t)dt < -\frac{1}{2T}\int_0^T (c_q(t) - c_{0\ \text{пор.}}(t))^2 dt, \quad (28)$$

або

$$Z_{\Delta\ \text{пор.}}(u) < -\frac{P_{\Delta\ \text{пор.}}}{2}, \quad (29)$$

де $P_{\Delta\ \text{пор.}}$ – потужність різницевого сигналу відносно порогового сигналу:

$$P_{\Delta\ \text{пор.}} = \frac{1}{T}\int_0^T c_{\Delta\ \text{пор.}}^2(t)dt, \quad (30)$$

$Z_{\Delta\ \text{пор.}}(u)$ – взаємна потужність сигналу на виході каналу та різницевого сигналу відносно порогового сигналу:

$$Z_{\Delta\ \text{пор.}}(u) = \frac{1}{T}\int_0^T u(t)c_{\Delta\ \text{пор.}}(t)dt. \quad (31)$$

Нерівність (30) характеризує стан невизначеності вирішальної схеми приймача. Тобто, якщо нерівність не виконується то це означає, що приймач фіксує ознаки небезпечного сигналу $c_q(t)$, який характеризується максимальними демаскуючими ознаками. Якщо ж нерівність виконується, то вирішальна схема приймає рішення не про відсутність ознак небезпечного сигналу, а про те, що вона не може виявити їх присутність або відсутність. Тобто, за умови надходження до приймача сигналів з рівнем менше порогового, завдяки власним шумам, цей приймач знаходиться у стані повної невизначеності.

Цей стан приймача називатимемо неможливістю його щодо впевненого виявлення ознак інформаційного сигналу. За цього стану приймач реально "не бачить" на вході ніяких сигналів, а "бачить" лише власні шуми. Вище сказане зручно зобразити за допомогою залежності станів приймача від значення корисного сигналу, що потрапляє на його вхід (рис. 6).

За нерівністю (29) можна збудувати вирішальну схему, що описуватиме умови неможливості впевненого виявлення та можливості впевненого виявлення ознак інформаційного сигналу за максимумом демаскування реалізацій інформаційних знаків (рис. 7).

На рис.6 та рис.7 рішення вирішальної схеми означають: y_0 – приймач не може впевнено виявити ознаки інформаційного сигналу. Цим самим забезпечено умову захищеності інформації від витоку – неможливості неконтрольованого поширення інформації по каналам витоку не може; y_q – приймач виявляє

ознаки небезпечного сигналу. Це є передумовою неконтрольованого поширення інформації по каналам витоку, інформація може бути перехопленою відповідними засобами, а тому ця умова є умовою ризику – інформація незахищена.

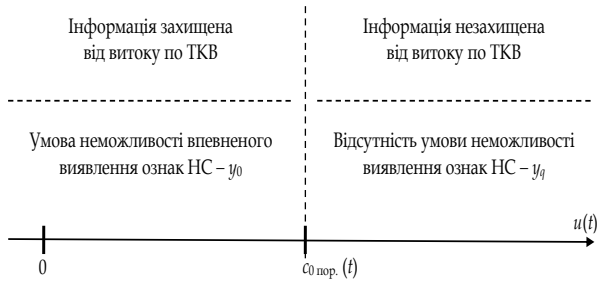

Рис. 6. Шкала стану приймача щодо визначення умови захищеності інформації – неможливості виявлення ознак за рівнем небезпечного сигналу з відмітками нульової реалізації та чутливості вимірювального приймача

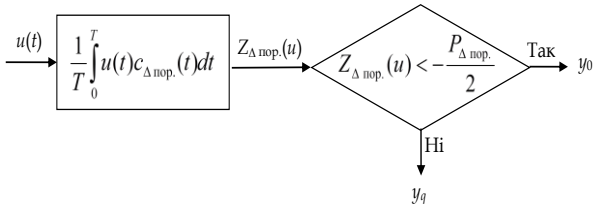

Рис. 7. Вирішальна схема оптимального приймача перехоплення з описом умов неможливості впевненого виявлення y0 та можливості впевненого виявлення yq ознак небезпечного сигналу за максимумом демаскування реалізацій інформаційних знаків

Як очевидно, імовірність щодо забезпечення неможливості впевненого виявлення ознак інформаційного сигналу при його виявленні формально можна виразити у виді:

$$p_{\text{нвос}} = p(y = y_0) = f(\text{сигнал}/\text{завада}). \qquad (32)$$

Імовірність ризику є імовірністю протилежної події:

$$p_R = p(y = y_q) = 1 - p_{\text{нвс}}. \qquad (33)$$

Таким чином, відповідно до стратегії детектування ознак інформаційного сигналу за максимумом їх демаскування обгрунтовано вирішальну схему оптимального приймача. Зазначена схема призначена для визначення умови захищеності дискретних джерел від неконтрольованого поширення інформації та оцінювання відповідної імовірності щодо наявності зазначеної умови.

Ця імовірність певним чином відповідає деякому ризику інформаційної безпеки, а тому може бути взятою як показник захищеності.

Отримана вирішальна схема дозволяє детектувати ознаки дискретного сигналу по одній з реалізацій, що мають максимальне демаскування, або перебувати в стані повної невизначеності щодо наявності цих ознак. Оскільки в стані невизначеності приймач "не бачить" інформаційних сигналів, то це дає впевненість, що він не може відтворювати і інформацію, що несе цей сигнал.

Висновки. Таким чином, запропоновано та обгрунтовано вирішальну схему оптимального приймача. На основі зазначеної вирішальної схеми отримано її приватний випадок, який описує умову неможливості впевненого детектування ознак дискретного сигналу в той час, коли ІКС або технічні засоби обробки та передачі інформації працюють. Дискретно-неперервний канал із використанням зазначеної схеми дозволяє імітувати середовище неконтрольованого поширення інформації, як для найгіршого випадку з точки зору захищеності, та знайти імовірність неможливості впевненого детектування ознак дискретного сигналу. Як очевидно, ця імовірність визначатиме імовірність ризику безпеки та може бути взятою як показник захищеності інформації від її неконтрольованого поширення в просторі.

Список літератури

[1]. Іванченко С.О., Некоз В.С. Унеможливлення виявлення ознак небезпечного сигналу як спосіб захисту інформації від витоку технічними каналами. Збірник наукових праць "Спеціальні телекомунікаційні системи та захист інформації". – К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2023. Вип. № 1 (37). С. 118-127.

[2]. Іванченко С.О., Некоз В.С. Обгрунтування критерію оптимальності прийому для побудови вирішальної схеми щодо виявлення ознак небезпечного сигналу. Збірник наукових праць "Спеціальні телекомунікаційні системи та захист інформації". К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2023. Вип. № 2 (38), С. 118-127.

[3]. Про державну таємницю : Закон України від 21 січ.1994 р. № 3855-XII.

[4]. Про інформацію : Закон України від 2 жовт. 1992 р. № 2657-XII.

[5]. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 лип. 1994 р. № 80/94-ВР.

[6]. Про затвердження Концепції технічного захисту інформації в Україні : Постанова Кабінету Міністрів України від 8 жовт. 1997 р. N 1126.

[7]. Батаєв О.П., Ковтун І.В., Корольова Н.А. Теорія електричного зв'язку : навч. посіб. Харків, 2010. 650 с.

УДК 004.056.53

Ivanchenko S., Nekoz V. Justification of the decision scheme for assessing the probability of detecting electromagnetic signals with the purpose of preventing their detection

Abstract. *The justification of the decision scheme for the construction of the receiver in order to realize the possible detection of signs of signals in space is carried out. In accordance with the condition regarding the impossibility of detecting signs of dangerous signals, the criterion of optimality is substantiated for the construction of the decisive scheme of the receiver. It is obtained by the maximum unmasking of information signals, pursuing the fulfillment of the security condition, as for the worst case. That is, if signals with more unmasking features, for example, power, are not detected, then signals with less unmasking features will not be detected either. On the basis of the obtained*

optimality criterion, a corresponding decision scheme of the optimal receiver is constructed. The proposed scheme considers three hypotheses: there are no signs of a signal, the impossibility of reliably determining the signs of a signal, and signs of a signal are present. On the basis of the specified decisive scheme, its special case is obtained, which describes the condition of the impossibility of reliably detecting the signs of a dangerous signal at the time when ICS or technical means of information processing and transmission are working. The discrete-continuous channel using the specified scheme allows to simulate the technical channel of information leakage, as for the worst case from the point of view of security, and to find the probability of the impossibility of reliably detecting the signs of a dangerous signal. Obviously, this probability will determine the probability of a security risk.

Keywords: *information security, cyber security, information and communication systems, information protection systems, information signal, discrete channel.*

Іванченко Сергій Олександрович, доктор технічних наук, професор, професор Спеціальної кафедри № 1 Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського".

Serhiy Ivanchenko, doctor of technical sciences, professor, professor of the Special Department No. 1 of the Institute of Special Communication and Information Protection of the National Technical University of Ukraine "Ihor Sikorskyi Kyiv Polytechnic Institute".

Некоз Василь Сергійович, викладач Спеціальної кафедри № 3 Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського".

Vasyl Nekoz, teacher of the Special Department No. 3 of the Institute of Special Communication and Information Protection of the National Technical University of Ukraine "Ihor Sikorskyi Kyiv Polytechnic Institute".

Отримано *21 травня 2024 року,* затверджено редколегією *26 червня 2024 року*