DOI: 10.18372/2410-7840.23.16770
УДК 004.4277.2.056.55

ПОКАЗНИКИ ЯКОСТІ ВИЯВЛЕННЯ ЛІТЕР АЛФАВІТУ СПЕЦІАЛІЗОВАНИМ ЗАСОБОМ ПЕРЕХОПЛЕННЯ ІНФОРМАЦІЇ З ЕКРАНІВ МОНІТОРІВ НА РІДКОКРИШТАЛЕВИХ СТРУКТУРАХ

Дмитро Євграфов, Юрій Яремчук

Розглянуто структурну схему сучасного засобу спеціальної розвідки, який дозволяє перехоплювати побічні електромагнітні випромінювання з екранів моніторів на рідкокристалевих структурах. Показано, що сучасні технології цифрового оброблення сигналів дозволяють реалізувати узгоджене приймання сигналів витоку інформації за допомогою цифрових фільтрів з гребеневою амплітудно-частотною характеристикою. Розглянуто спектральне подання сигналів витоку інформації з екранів моніторів, на яких висвітлюється одна з літер українського алфавіту. Доведено, що навіть для малої розрізняльної спроможності спектрального подання літер вони мають характерний вигляд. Знайдено дисперсію на виході лінійної системи спеціалізованого засобу розвідки, яка в сотні разів менша за дисперсію звичайного широкосмугового приймача сигналів. Змодельований вигляд перехоплених з екрану монітору на рідкокристалевих структурах літер алфавіту для різних співвідношень сигнал/шум на виході лінійної системи приймача спеціалізованого засобу розвідки. Знайдено ймовірності хибної тривоги під час виявлення сигналів витоку інформації, залежно від нормованого порогу виявлення. Для фіксованого нормованого порогу виявлення розраховано ймовірності правильного виявлення тієї, або іншої літери українського алфавіту на фоні внутрішніх шумів спеціалізованого засобу розвідки. Для фіксованого співвідношення сигнал/шум і фіксованої хибної тривоги знайдено ймовірності правильного виявлення різних літер українського алфавіту.

Ключові слова: *побічні електромагнітні випромінювання і наведення, екрани на рідкокристалевих структурах, коефіцієнти Фур'є спектру витоку інформації, спеціалізований засіб розвідки, імовірність хибної тривоги, імовірність правильного виявлення.*

ВСТУП

З моменту опублікування праці Маркуса Куна, в якій він уперше дослідив витік інформації з моніторів на рідкокристалевих структурах (РКС), пройшло шістнадцять років [1]. Цей час розвинені промислові країни використали для створення спеціальних засобів розвідки (СЗР), здатних перехоплювати інформацію на відстанях у десятки-сотні метрів [2, 3]. При цьому більшість відкритих публікацій на цю тему базуються на бажанні одразу ж описати пристрої перехоплення інформації, витік якої обумовлений побічними електромагнітними випромінюваннями і наведеннями (ПЕМВІН), без обґрунтування їх структури із застосуванням класичної теорії оптимальної фільтрації сигналів. Насправді приймач СЗР сигналів витоку інформації як з екранів моніторів на електронно-променевих трубках (ЕПТ), так і з екранів на РКС має просту структуру, обґрунтовану [4]. СРЗ має складатися (див. рис. 1) з антенної системи (А), підсилювача високої частоти з гребінковим фільтром (ПВЧ з ГФ), підсилювача – формувача відеосигналів (П-Ф), генератора кадрових імпульсів (Г), формувачів кадрової і строкової розгорток (ФКР) і (ФСР), регульованої лінії затримки (РЛЗ), електронно-променевої трубки з відхиляючою системою. Антенна система (А) приймає сигнал з монітору на РКС, який підсилюється у ПВЧ з ГФ. Зі спектру сигналу гребінковим фільтром обираються лише інформативні частоти, які кратні частоті вертикальної розгортки монітору – джерела витоку інформації f_{ver}, і придушуються ті складові спектру, які додають шумової компоненти сигналу. Оскільки верхня гранична частота витоку інформації сягає 2 ГГц, для мінімальної $f_{ver} = 60$ Гц кількість гребінців ПВЧ з ГФ сягатиме $K = 3{,}33 \cdot 10^7$.

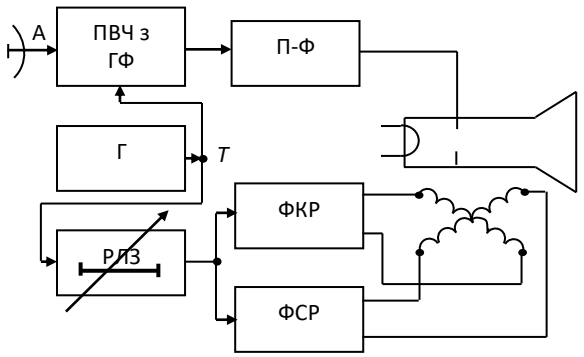


Рис. 1 Структурна схема СЗР перехоплення інформації з екрану монітору

Для підвищення контрастності сигналу він подається на модулюючий електрод через П-Ф сигналів, який може працювати як підсилювач-обмежувач, або формувач фронтів сигналу. Синхронізує роботу пристрою перехоплення Г, який через ФКР і ФСР формує відповідні напруги відхилення електронно-променевої трубки. Оскільки момент початку кадрової розгортки є невідомим повної синхронізації зображень на екрані з РКС і ЕПТ пристрою перехоплення досягається регульованою лінією затримки. Зрозуміло, що схема рис. 1 подана у вигляді, що спрощує розуміння принципів роботи СРЗ. Насправді всі його елементи можуть бути частинами мікропроцесорного пристрою з відображенням інформації на сучасних моніторах.

Засіб поданий на рис. 1 є причиною, з якої фахівці із захисту інформації мають непокоїтися. І незважаючи на існуючи методики, які обґрунтовують небезпечні напруженості магнітних і електричних полів поблизу монітору на РКС, без ґрунтовного осмислення того, які саме спектральні складові ПЕМВІН є важливими, створити ефективну систему захисту неможливо.

ПОСТАНОВКА ЗАДАЧІ

Поставимо перед собою просту задачу. Припустимо, що противник за допомогою засобу рис. 1 намагається перехопити з нашого монітору на РКС текстову інформацію. Для спрощення вважатиме, що картинка на екрані монітору протягом тривалого часу аналізу $t_{\text{а}}$ є статичною (самий гірший для нас випадок). Обмежимося тут і розглядом максимально контрастних текстів, наприклад чорних літер на білому фоні екрану. І, нарешті, ускладнимо задачу тим, що на усьому екрані монітору висвітлюється лише одна з 33 літер українського алфавіту.

Дамо собі відповідь на просте питання: з якою імовірністю противник здатній виявити літеру “Л”, або “Ж” [5], для певного фіксованого співвідношення сигнал/шум на виході лінійної частини приймача СРЗ? Вважатиме, що ПЕМВІН розглядається на фоні лише внутрішніх шумів приймача СРЗ. Подібні дослідження дають можливість не лише оцінити імовірності витоку інформації з екрану моніторів на РКС, а і впевнитися у надійності існуючих методик, після урахування промислових і природніх завад радіочастотного спектру.

Актуальність задачі полягає в осмисленні реальних можливостей сучасних СЗР, якими володіє противник, максимально узгоджених з сигналами ПЕМВІН і такими, що дають можливість витягнути інформацію з вкрай малопотужних джерел витоку.

Приведені дослідження зробимо для кадру на екрані монітора, який складається з h - строк по w пікселів кожний, тобто той, що має $w\times h$ пікселів з типорозміром 1024×768. Зрозумівши логіку викладеного матеріалу можна легко поширити подібні дослідження на інші типорозміри. Крім того, дослідимо тут лише літери українського алфавіту найбільш поширених шрифтів Arial і Times New Roman.

МЕТА РОБОТИ

Відшукати показники якості виявлення окремих літер українського алфавіту приймачем СРЗ противника, залежно від співвідношень сигнал/шум на виході його лінійної частини.

Спектральне подання сигналів витоку інформації з екрану монітору

Оскільки обробка сигналів в сучасному СЗР передбачатиме побудову ПВЧ з ГФ у вигляді цифрового фільтру бажано подати растрове зображення на екрані монітору у спектральному вигляді. Відповідно до розглянутої в роботі [6] часової моделі сигналів витоку $C(t)$, $0\le t\le T_{\text{к}}$, де $T_{\text{к}}=1/f_{ver}$, модулі коефіцієнтів ряду Фур’є:

$$S(k)=\frac{1}{T_{\text{к}}}\left|\int_0^{T_{\text{к}}}C(t)\exp\left(-j\frac{2\pi kt}{T_{\text{к}}}\right)dt\right|,k=1,2,..K,\ (1)$$

повністю описують будь-яку інформацію на екрані монітору, що складається з h інформаційних строк по w пікселів тривалістю $\tau_{\text{п}}$, які повторюються з періодом $T_{\text{с}}$.

Якщо подати інформацію на екрані монітору двовимірною матрицею $C_{i,m}$, $i=0,1,..,h-1$ – поточна стрічка растрового зображення, $m=0,1,..,w-1$ – поточне знакомісце у стрічці, то сигнал витоку можна записати у вигляді:

$$C(t)=\sum_{i=0}^{h-1}\sum_{m=0}^{w-1}C_{i,m}\left[\mathbf{1}(m\tau_{\text{п}}+\tau_{\text{п}}+iT_{\text{с}}-t)-\mathbf{1}(m\tau_{\text{п}}+iT_{\text{с}}-t)\right],$$

де $\mathbf{1}(x)$– одинична функція, а модулі коефіцієнтів (1) – розрахувати за виразом:

$$S(k)=\frac{1}{2\pi k}\left|j\sum_{i=0}^{h-1}\sum_{m=0}^{w-1}C_{i,m}\left[\exp\left(-\frac{j2\pi k\left(m\tau_{\text{п}}+\tau_{\text{п}}+iT_{\text{с}}\right)}{T_{\text{к}}}\right)-\right.\right. \quad (2)$$
$$\left.\left.-\exp\left(-\frac{j2\pi k\left(m\tau_{\text{п}}+iT_{\text{с}}\right)}{T_{\text{к}}}\right)\right]\right|$$

Для зазначеного типорозміру екрану з $w=1024$ и $h=768$ режиму XGA ($f_{ver}=60$ Гц) у виразі (2): $T_{\text{к}}=16{,}667$ мс, $T_{\text{с}}=20{,}661$ мкс, $\tau_{\text{п}}=0{,}0154$ мкс.

На рис. 2 з розрізняльною здатністю в 0,1 МГц у логарифмічній шкалі проілюстровано спектральне подання літери "Ю", на рис. 3 – літери "Ж", а на рис. 4 – літери "І", розраховані відповідно до (2) в додатку Mathcad версії 14.0, з використанням команди READBMP("data.bmp"). Для цього відповідні літери висотою у 500 кегель шрифту Arial редактору World були переведені у графічні зображення data.bmp.

Використання модулів коефіцієнтів Фур'є дозволяє досягнути індиферентності від місцеположення літери на екрані монітору, закладеного у фазових характеристиках спектру. Бачимо, що кожна літера має свій власний спектральний малюнок, навіть за умови низької розрізняльної здатності. Як і слід було очікувати, чим ширше літера від "І" до "Ю" та "Ж" шрифту Arial, тим більша частина спектру зосереджена на менших частотах сигналу витоку.

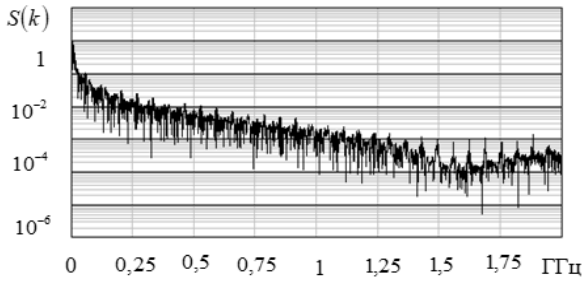


Рис. 2. Спектральне подання літери "Ю"

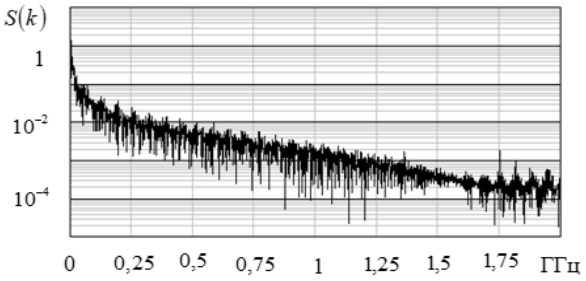


Рис. 3. Спектральне подання літери "Ж"

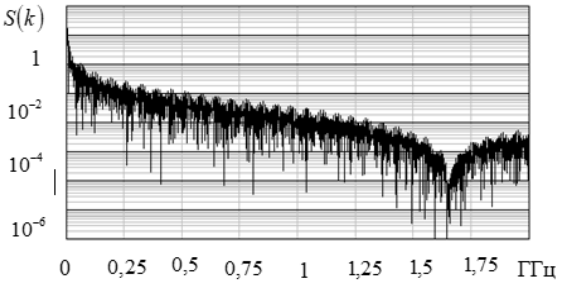


Рис. 4. Спектральне подання літери "І"

Розв'язання задачі в умовах апріорної невизначеності щодо типу і розміру шрифту

Припустимо, що нам відоме значення f_{ver} монітору – джерела ПЕМВІН, а СЗР передбачає лише оптимізацію лінійного тракту шляхом цифрової фільтрації (ЦФ) з амплітудно-частотною характеристикою (АЧХ) тракту ПВЧ з ГФ, поданого на рис. 1.

Після антенного широкосмугового підсилювача сигналів він може одразу ж оцифровуватися з частотою дискретизації $f_{\text{д}}=f_{ver}K$ (періодом дискретизації $T=1/f_{\text{д}}$), оскільки сучасні SDR-технології дозволяють будувати лінійні тракти зі смугами до $\Delta f_{\text{лт}}=3$ ГГц (при $f_{\text{д}}=6$ ГГц).

Для ЦФ другого порядку з гребінковим АЧХ із K гребенями, симетричними відносно інформативних частот $f_{ver}k$, $k=1,2,..K$:

$$C(\omega)=\left|\frac{A\left(1-\exp\left(-2j\omega TK\right)\right)}{1+A-2\exp\left(-j\omega TK\right)+\left(1-A\right)\exp\left(-2j\omega TK\right)}\right|= \quad (3)$$
$$=\frac{A}{\sqrt{\frac{1-\cos\left(\omega TK\right)}{1+\cos\left(\omega TK\right)}+A^2}}$$

де

$$A=\text{tg}\left(\frac{\pi\Delta f_{\text{гр}}}{f_{ver}}\right) \quad (4)$$

$\Delta f_{\text{гр}}=1/t_{\text{а}}\le f_{ver}/2$ – ефективна смуга перепускання гребінця ПВЧ з ГФ, структурна схема подана на рис. 5.

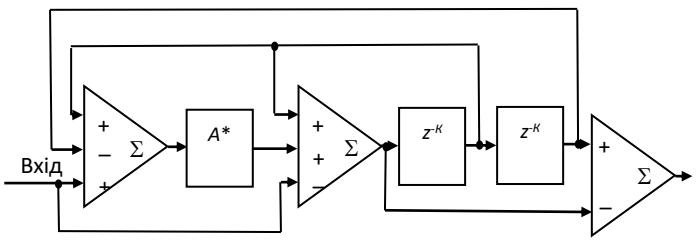


Рис. 5 Структурна схема ЦФ, що реалізує АЧХ ПВЧ з ГФ

Коефіцієнт A^* в схемі розраховується відповідно до виразу:

$$A^* = \frac{1-A}{1+A},$$

де A – задано (4).

Якщо б приймання сигналу відбувалося би звичайним приймачем зі широкосмуговим лінійним трактом для усіх спектральних складових ПЕМВІН, ефективний спектр яких становить $\Delta f_{лт} \approx 2\,\text{ГГц}$, дисперсія на його виході дорівнювала би:

$$\sigma^2 = N_0 \Delta f_{лт},$$

N_0 – однобічна спектральна густина потужності шуму. Використання же ПВЧ з ГФ призводять до набагато менших дисперсій на виході лінійної частини приймача, яку можна подати з урахуванням (3) і (4) у вигляді:

$$\sigma^2_{гр} = N_0 \int_0^{\Delta f_{лт}} C^2(2\pi f)\, df = \frac{N_0 \Delta f_{лт} \operatorname{tg}\left(\pi \Delta f_{гр} / f_{ver}\right)}{1+\operatorname{tg}\left(\pi \Delta f_{гр} / f_{ver}\right)}, \quad (5)$$

оскільки $\dfrac{\operatorname{tg}\left(\pi \Delta f_{гр} / f_{ver}\right)}{1+\operatorname{tg}\left(\pi \Delta f_{гр} / f_{ver}\right)} << 1$, для малих $\Delta f_{гр}$ (великих t_a).

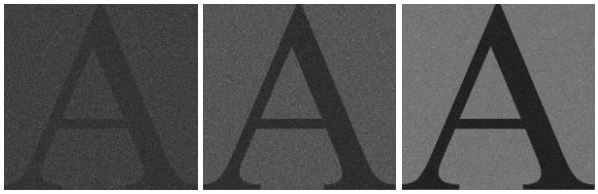
Наприклад, якщо зображення на екрані не змінюється $t_a = 5\,\text{с}$, $\Delta f_{гр} = 0{,}2\,\text{Гц}$, а для $f_{ver} = 60\,\text{Гц}$ $\sigma^2_{гр}$ менше σ^2 у сто разів, що робить відповідні співвідношення сигнал/шум для кожної інформаційної гармоніки у стільки же разів більшими. Саме завдяки цьому деструктивна енергія шуму приймача СЗР найменше викривлятиме інформативні складові ПЕМВІН.

Приймач СРЗ обробляє сигнали витоку і відновлює перехоплене зображення літери на власному моніторі. На рис. 6 подано перехоплене зображення літери "А" шрифту Times New Roman при співвідношеннях сигнал/шум (по напрузі) $q = a/\sigma_{гр} = 1; 2; 4$. Чорно-біле зображення літери отримані моделюванням процесу накладання на растровий сигнал, кожний піксель якого поданий одним байтом для амплітуд $a_{i,m}$ від 0 (чорний колір пікселю) до 255 (білий колір пікселю), шумового сигналу з відповідними середніми квадратичними відхиленнями $\sigma_{гр} = 255; 127; 63$. Формування кожного пікселю зображення літери на фоні шуму відбувалося у середовищі Mathcad відповідно до виразу:

$$A_{i,m} = \sqrt{\left(\frac{a_{i,m}}{\sqrt{2}} + n_c\right)^2 + \left(\frac{a_{i,m}}{\sqrt{2}} + n_s\right)^2}, \quad (6)$$

n_c, n_s – незалежні квадратурні відліки білого гаусовського шуму з нульовим середнім і дисперсією $\sigma^2_{гр}$, які формувалися за допомогою команди $\text{rnorm}(w \cdot h, 0, \sigma_{гр})$.

Надалі розрахований відповідно до (6) сигнал нормувався до максимального значення у 255 і перетворювався за допомогою команди WRITEBMP("data.bmp") у файл графічного зображення, який і поданий на рис. 6 а, для $q = 1$, на



а) *б*) *в*)

Рис. 6 Вигляд літери "А" на екрані СЗР: *а*) – для (q); *б*) – для (6); *в*) – для (e)

Теорію для показників виявлення сигналів на екрані СЗР надано у [7]. Імовірність хибної тривоги β розраховується через розподілення абсолютного максимуму релеєвського стаціонарного процесу. Якщо для виявлення тієї або іншої літери прийнятій після фільтрації в ПВЧ з ГФ сигнал подається на амплітудний детектор, а обгинаюча сигналу порівнюється з порогом h, імовірність перевищення за час t_a післядетекторним процесом (без корисного сигналу), нормованого відносно $\sigma_{гр}$ порога $h_0 = h/\sigma_{гр}$, становить:

$$\beta = 1 - \left(1 - \exp\left(-\frac{h_0^2}{2}\right)\right) \cdot \exp\left[-\frac{\sqrt{\frac{\omega_2}{2\pi}} \cdot h_0 \cdot \exp\left(-\frac{h_0^2}{2}\right)}{1-\exp\left(-\frac{h_0^2}{2}\right)} \cdot t_a\right], \quad (7)$$

ω_2 – другий спектральний момент процесу, який на виході лінійної системи ПВЧ з ГФ, з урахуванням (3) і (4), можна порахувати відповідно до виразу:

$$\omega_2 = \frac{\int_0^{2\pi\Delta f_{лт}} \omega^2 C^2(\omega)\, d\omega}{\int_0^{2\pi\Delta f_{лт}} C^2(\omega)\, d\omega} \approx \frac{4\pi^2 \Delta f_{лт}^2}{3}, \quad (8)$$

для будь якого не дуже малого A.

Залежність імовірності хибної тривоги β від нормованого порогу h_0, розраховану відповідно до (7), з урахуванням (8), для $\Delta f_{\text{лт}} = 2\,\text{ГГц}$ і $t_{\text{а}} = 5;20;60\,\text{с}$, подано на рис. 7. За допомогою цих залежностей для фіксованої за критерієм Неймана-Пірсона імовірності β, відшукується нормований поріг виявлення h_0.

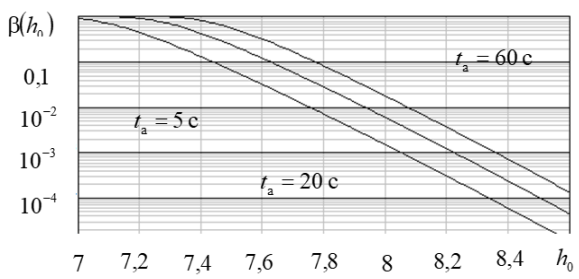


Рис. 7. Залежність імовірності хибної тривоги від нормованого порогу

Імовірність пропуску сигналу α за час t виявлення тієї, або іншої літери $0 \le t \le t_{\text{а}}$, можна порахувати через розподілення абсолютного максимуму райсовського нестаціонарного процесу:

$$\alpha = \int_0^{h_0} x \exp\left(-\frac{x^2}{2} - \frac{q^2(0)}{2}\right) I_0[xq(0)]dx \cdot$$
$$\cdot \exp\left[-\int_0^{t_{\text{а}}} \frac{\sqrt{\frac{\omega_2}{2\pi}} h_0 \exp\left(-\frac{h_0^2}{2} - \frac{q^2(t)}{2}\right) I_0[h_0 q(t)]}{\int_0^{h_0} x \exp\left(-\frac{x^2}{2} - \frac{q^2(t)}{2}\right) I_0[xq(t)]dx} dt\right], \quad (9)$$

де $I_0[x]$ – модифікована функція Беселя нульового порядку, $q(t)$, $0 \le t \le t_{\text{а}}$ – співвідношення напруги сигналу витоку інформації до середньо квадратичного відхилення шуму на виході ПВЧ з ГФ.

На рис. 8 подані розраховані відповідно до (9), з урахуванням (8), залежності ймовірностей правильного виявлення $1-\alpha$ літер "І", "Д" та "Ш" шрифту Times New Roman, від співвідношень $q_0 = \max\limits_{0 \le t \le t_{\text{а}}} q(t)$, для $t_{\text{а}} = 5\,\text{с}$ і $h_0 = 8{,}045$, що задає $\beta = 10^{-3}$.

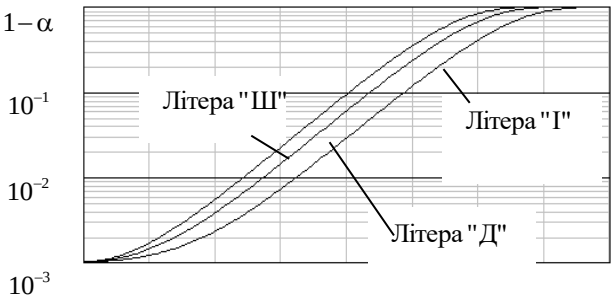


Рис 8. Ймовірності правильного виявлення, для $t_{\text{а}} = 5\,\text{с}$

У табл. 1 подано залежності виявлення літер українського алфавіту шрифту Times New Roman для $q = 1$ на виході СЗР, $t_{\text{а}} = 60\,\text{с}$ і фіксованого $\beta = 10^{-3}$.

У табл. 2 ті ж дані подані для $q = 1{,}5$. Як і слід було очікувати, ті літери, що мають більшу площу пікселів білого кольору – виявляються краще, а ймовірності правильного виявлення збільшуються (зміщуються ліворуч).

З енергетичної точки зору це не викликає жодних заперечень.

Таблиця 1

Ймовірності виявлення літер українського алфавіту СЗР, для $q = 1$

А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М
0,197	0,127	0,136	0,146	0,143	0,15	0,158	0,213	0,109	0,166	0,039	0,05	0,134	0,164	0,173	0,204

Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
0,168	0,162	0,172	0,127	0,162	0,155	0,191	0,172	0,186	0,147	0,163	0,22	0,195	0,131	0,228	0,159

Таблиця 2

Ймовірності виявлення літер українського алфавіту СЗР, для $q = 1{,}5$

А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М
0,998	0,979	0,998	0,988	0,987	0,99	0,992	0,999	0,962	0,994	0,666	0,764	0,983	0,994	0,995	0,998

Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
0,998	0,994	0,995	0,978	0,993	0,992	0,998	0,995	0,997	0,989	0,994	0,999	0,998	0,981	0,999	0,992

Проте, у цьому процесі виявлення не використовуються алгоритми узгодженого приймання сигналів витоку для конкретних шрифтів конкретного розміру, які дають набагато кращі показники якості виявлення літер.

ВИСНОВКИ

1. Існують усі умови для створення в Україні спеціалізованих засобів розвідки з використанням як цифрової фільтрації сигналів, так і оптимальних алгоритмів їх оброблення, здатних перехоплювати витік інформації з моніторів на рідкокришталевих структурах.

2. Спектри сигналів витоку текстової інформації з екранів моніторів мають характерну структуру для кожної літери на екрані монітору.

3. Інформація про окремі літери українського алфавіту, яка накопичується протягом хвилини зі співвідношеннями сигнал/шум $q=1{,}5$ на виході лінійної частини спеціалізованого засобу розвідки, перехоплюється з імовірністю від 0,666 до 0,999, для імовірності хибної тривоги $\beta=10^{-3}$.

4. У подальшому корисно розв'язати задачу з якою імовірністю розрізняється, наприклад, літера "О" від літери "С", або "І" від "Ї".

ЛІТЕРАТУРА

[1] Markus G. Kuhn. Security Limits of Compromising Emanations // *Cryptographic Hardware and Embedded Systems: Journal.* – 2005. – Vol. 3659. – pp. 265-279.

[2] Наконечний Т.А., Євграфов Д.В. Перехоплення сигналу витоку інформації з екрану монітора. *Міжнародна науково-технічна конференція «Радіотехнічні поля, сигнали, апарати та системи». Радіотехнічний факультет НТУУ КПІ імені Ігоря Сікорського*, 18-24 листопада 2018 року, м. Київ, Україна. С. 279-281.

[3] Tanaka Hidema, Takizawa Osamu, Yamamura Akihiro. A Trial of the interception of Display image using Emanation of Electromagnetic Wave // *Journal. 2005*. – Vol. 34, no. 2. – pp. 147-155.

[4] Євграфов Д.В. *Фізичні основи захисту інформації в радіоелектронній апаратурі*: навч. посіб. / Д.В. Євграфов . – К.: НТУУ «КПІ», 2014. – 176 с. – Бібліогр.: С. 170-172.

[5] Yevgrafov D. V. *Signal detection by means of electronic intelligence*: monograph. Kyiv: Publish house "Con dor", 2020. - 152 p.

[6] Євграфов Д.В., Яремчук Ю.Є. Розрахункові спектри сигналів витоку інформації з екранів моніторів на рідкокришталевих структурах. К.: *Інститут проблем реєстрації інформації НАН України*, № 2, Том 23, С. 3-12. 2021.

[7] Євграфов Д.В. *Розподілення абсолютного максимуму випадкового поля в теорії аналізу радіотехнічних систем*: монографія / Д.В. Євграфов. – Київ: КПІ ім. Ігоря Сікорського, вид-во «Політехніка», 2021. – 276 с.

ПОКАЗАТЕЛИ КАЧЕСТВА ОБНАРУЖЕНИЯ БУКВ АЛФАВИТА СПЕЦИАЛИЗИРОВАННЫМ СРЕДСТВОМ ПЕРЕХВАТА ИНФОРМАЦИИ С ЭКРАНОВ МОНИТОРОВ НА РЕДКОКРИСТАЛЛИЧЕСКИХ СТРУКТУРАХ

Рассмотрено структурную схему современного средства специальной разведки, который позволяет перехватывать побочные электромагнитные излучения с экранов мониторов на редкокристаллических структурах. Показано, что современные технологии цифровой обработки сигналов позволяют реализовать согласованный прием сигналов утечки информации при помощи цифровых фильтров с гребеньковой амплитудно-частотной характеристикою. Рассмотрено спектральное представление сигналов утечки информации с экранов мониторов, на которых высвечивается одна из букв украинского алфавита. Доказано, что даже для малой разрешающей способности спектрального представления букв они имеют характерный вид. Найдено дисперсию на выходе линейной системы специализированного средства разведки, которая в сотни раз меньше дисперсии обычного широкополосного приемника сигналов. Смоделирован вид перехваченных с экрана монитора на редкокристаллических структурах букв алфавита для разных отношений сигнал/шум на выходе линейной системы приемником специализированного средства разведки. Найдены вероятности ложной тревоги во время обнаружения сигналов утечки информации, в зависимости от нормированного порогу обнаружения. Для фиксированного нормированного порога обнаружения рассчитаны вероятности правильного обнаружения той, или иной буквы украинского алфавита на фоне внутренних шумов специализированного средства разведки. Для фиксированного соотношения сигнал/шум и фиксированной ложной тревоги найдены вероятности правильного обнаружения разных букв украинского алфавита.

Ключевые слова: побочные электромагнитные излучения и наведения, экраны на редкокристаллических структурах, коэффициенты Фурье спектра утечки информации, специализированное средство разведки, вероятность ложной тревоги, вероятность правильного обнаружения.

INDICATORS OF THE QUALITY OF DETECTION OF LETTERS OF THE ALPHABET BY A SPECIALIZED MEANS OF INTERCEPTING INFORMATION FROM MONITOR SCREENS ON RARE-CRYSTAL STRUCTURES

The block diagram of a modern means of special reconnaissance, which allows intercepting spurious electromagnetic radiation from monitor screens on rare-crystal struc-

tures, is considered. It is shown that modern digital signal processing technologies make it possible to implement coordinated reception of information leakage signals using digital filters with a comb amplitude-frequency characteristic. The spectral representation of information leakage signals from monitor screens, on which one of the letters of the Ukrainian alphabet is displayed, is considered. It is proved that even for a low resolution of the spectral representation of letters, they have a characteristic form. The dispersion at the output of the linear system of a specialized reconnaissance means was found, which is hundreds of times less than the dispersion of a conventional broadband signal receiver. The view of the letters of the alphabet intercepted from the monitor screen on rare-crystal structures for different signal-to-noise ratios at the output of the linear system by the receiver of a specialized reconnaissance tool is modeled. The probabilities of false alarms are found during the detection of information leakage signals, depending on the normalized detection threshold. For a fixed normalized detection threshold, the probabilities of correct detection of one or another letter of the Ukrainian alphabet against the background of internal noises of a specialized reconnaissance means are calculated. For a fixed signal-to-noise ratio and a fixed false alarm, the probabilities of correct detection of different letters of the Ukrainian alphabet are found.

Keywords: purious electromagnetic radiation and guidance, screens on rare-crystal structures, Fourier coefficients of the spectrum of information leakage, specialized reconnaissance means, probability of false alarm, probability of correct detection.

Яремчук Юрій Євгенович, директор Центру інформаційних технологій та захисту інформації, професор кафедри менеджменту та безпеки інформаційних систем Вінницького національного технічного університету.

E-mail: yurevyar@vntu.edu.ua.

Orcid ID: 0000-0002-6303-7703.

Яремчук Юрий Евгеньевич, директор Центра информационных технологий и защиты информации, профессор кафедры менеджмента и безопасности информационных систем Винницкого национального технического университета.

Yaremchuk Yurii, Director of the Center for Information Technologies and Information Protection, Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University.

Євграфов Дмитро Вікторович, здобувач Вінницького національного технічного університету наукового ступеня доктора технічних наук за спеціальністю 125 «Кібербезпека».

E-mail: ramgraf@bigmir.net.

Orcid ID: 0000-0001-9651-1558.

Евграфов Дмитрий Викторович, соискатель Винницкого национального технического университета научной степени доктора технических наук по специальности 125 «Кибербезопасность».

Evgrafov Dmitry, candidate of Vinnytsia National Technical University for the degree of Doctor of Technical Sciences, specialty 125 "Cybersecurity".