УДК 621.373

В.Б. Дудикевич[1], І.С. Собчук[1], Л.М. Ракобовчук[1], В.С. Зачепило[2]

[1]*Національний університет «Львівська політехніка», Львів*
[2]*ЗРННЦЗІ, Львів*

ДОСЛІДЖЕННЯ ПОБІЧНОГО ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЕННЯ ВІД ФЛЕШ НОСІЇВ

В даній роботі зроблений огляд проблем виникнення електромагнітного випромінювання від засобів електронно-обчислювальної техніки. Проведено аналіз інформації, що обробляється за допомогою засобів електронно-обчислювальної техніки. Значну увагу приділено аналізу та опису технічних каналів витоку інформації, вибір наявних засобів захисту інформації. В роботі описано принцип роботи та методика вимірювання побічного електромагнітного випромінювання та наводів за допомогою автоматизованого комплексу АКОР-2ПК.

В завершальній частині проведено дослідження та порівняльну характеристику вимірювання електромагнітного випромінення від флеш носіїв за допомогою АКОР-2ПК.

Ключові слова: *побічні електромагнітні випромінювання та наводи, ПЕМВН.*

Вступ

Сучасні методи обробки інформації, що містять державну таємницю або комерційні, технологічні секрети, проходить етап обробки на персональних комп'ютерах. Засобам ЕОМ: флеш носії, магнітні диски, принтери, клавіатура та інші властиві випромінювання ПЕМВН. Інформація в цих пристроях передається послідовним кодом, всі параметри цього коду стандартизовані і добре відомі [1, 3, 7].

Основний матеріал

Перехоплення електромагнітних випромінювань базується на широкому використанні найрізноманітніших радіоприймальних засобів, засобів аналізу і реєстрації інформації та інших (антенні системи, широкосмугові антенні підсилювачі, панорамні аналізатори та ін.), які як правило розміщені за межами контрольованого периметра, що створює проблеми з виявлення таких пристроїв.

Також ведеться перехоплення і інших електромагнітних випромінювань, таких як радіолокаційні, радіонавігаційні системи, системи управління, а також перехоплення електромагнітних сигналів, що виникають в електронних засобах за рахунок самозбудження, акустичного впливу, паразитних коливань і навіть сигналів ПЕОМ, що виникають при видачі інформації на екран. Слід зазначити, що перехоплення інформації має ряд наступних особливостей в порівнянні з іншими способами добування інформації:

• інформація видобувається без безпосереднього контакту з джерелом;

• на прийом сигналів не впливають ні час року, ні час доби;

• інформація виходить в реальному масштабі часу, в момент її передачі та випромінювання;

• добування ведеться таємно, джерело інформації часто і не підозрює, що його прослуховують;

• дальність прослуховування обмежується тільки особливостями поширення радіохвиль відповідних діапазонів.

Дальність перехоплення сигналів, наприклад ПЕОМ, можна характеризувати показниками, які враховують конструктивні особливості ЕОМ та антенних систем перехоплення табл. 1. [9].

Таблиця 1

Дальність перехоплення сигналів

Характеристики антен	Корпус ПЕОМ	
	пластмасовий	металевий
Ненаправлена	50 м	10 м
Направлена	1000 м	200 м

Електромагнітне екранування приміщень у широкому діапазоні частот є складним технічним завданням, вимагає значних капітальних витрат, постійного контролю і не завжди можливо з естетичним та ергономічним міркувань.

Для здійснення активного радіотехнічного маскування ПЕМВН використовуються пристрої, що створюють шумове електромагнітне поле в діапазоні частот від декількох кГц до 1000 МГц. Для цих цілей використовуються надширокосмугові передавачі Базальт-5ГЕШ та ВОЛНА-4Р, які мають сертифікат відповідності ДССЗЗІ України [2, 3]..

До недавнього часу на вітчизняному ринку та ринку країн СНД були представлені такі комплекси для вимірювання ПЕМВН:

Пристрій	Діапазон рабочих частот, МГц	Виробник
SMV-8,5	26–1000	Messelecktronik, Німеччина
SMV-11	0,009–30	— " —
SMV-41	0,009–1000	— " —
—Элмас"	30–1300	ПО –Вектор", С.–Петербург
ESH-2	0,009–30	RHODE & SHWARZ, ФРН
ESV	20–1000	— " —
ESH-3	0,009–30	— " —
ESVP	20–1300	— " —
АКОР-2ПК	0,00001-3000	НТЦ –КВАНТ— Україна

Вимірювальні приймачі (ЕЛМАС, ESH-3, ESVP, SMV-41, АКОР-2ПК) автоматизовані та обладнані інтерфейсами за стандартом IEEE-488, що дає можливість керувати режимами роботи приймача за допомогою зовнішньої ЕОМ.

Сучасні аналізатори спектру з вбудованими мікропроцесорами дозволяють аналізувати різні параметри сигналів. Є можливість об'єднання аналізатора спектра за допомогою інтерфейсу з іншими вимірювальними приладами і зовнішньої ЕОМ в автоматизовані вимірювальні системи, до таких систем відноситься АКОР-2ПК [11 – 15].

Цифровий комплекс вимірювання ПЕМВН реалізований на основі автоматизованого комплексу виявлення радіовипромінювань АКОР-2ПК являє собою аналізатор спектру та високочутливий селективний вимірювальний приймач для частотного діапазону від 10 Гц до 3000 МГц.

Комплекс забезпечує:

– вимірювання напруги, створюваного ПЕМВН від різних пристроїв низькострумової техніки (персональних ЕОМ, оргтехніки, апаратури зв'язку);

– вимірювання напруженості електричного **(Е)** і магнітного **(Н)** поля (при підключенні вимірювальних антен);

– вимірювання струму (при підключенні вимірювального струмознімача).

Комплекс забезпечує виконання наступних основних і додаткових функцій:

Основні функції:

– вимірювання квазіпікового значення регулярних імпульсних сигналів;

– вимірювання амплітудного та середнього значень модульованих сигналів;

– вимірювання амплітудного, середнього амплітудного та середнього значень регулярних імпульсних сигналів;

– вимірювання середньоквадратичного значення шумів.

Додаткові функції:

– аналіз спектральних характеристик вимірювальних сигналів;

– аналіз амплітудно-тимчасових характеристик імпульсних сигналів;

– аналіз фазових характеристик сигналів;

– прослуховування демодульованого сигналу з різними видами модуляції;

– запис частот і рівнів вимірювальних сигналів на жорсткий диск ПЕОМ з подальшим їх виводом;

– введення значень коефіцієнтів калібрування вимірювальних електричних і магнітних антен і струмознімача;

– протоколювання результатів вимірювань;

– протоколювання результатів визначення похибки вимірювання рівнів сигналів.

Схема електричних з'єднань вимірювального тракту вимірювача наведена на рис. 1.

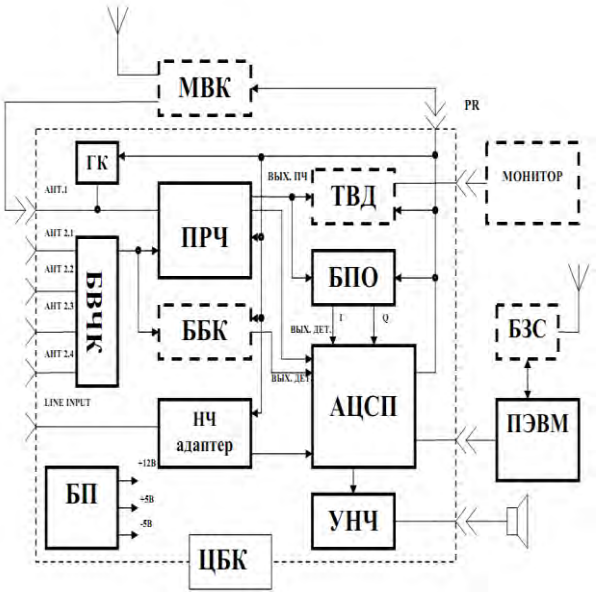

Рис. 1. Схема електричних з'єднань комплексу

На схемі позначено:

• **ЦБК** – основний блок вимірювача;

• **БПО** – блок панорамного огляду і квадратурної обробки сигналу;

• **ПРЧ** – перетворювач радіочастот;

• **БП** – вбудований блок живлення апаратурної частини ЦПК від мережі 220В;

• **АЦСП** – аналого-цифровий сигнальний процесор;

• **ТВД** – блок телевізійних детекторів;

• **ГК** – блок генератора калібрування;

• **ПЭВМ** – персональний комп'ютер;

• **ББК** – блок безшумної кореляції;

• **БВЧК** – блок високочастотного комутатора;

• **НЧ**-адаптер – низькочастотний адаптер;

• **УНЧ** – підсилювач низької частоти;

• **БЗС** – блок зондуючого сигналу;

• **МВК** – мікрохвильовий конвертер;

Кабелі підключення апаратурної частини вимірювача до ПЕОМ Notebook:

• кабель **USBA-USBB**. Підключає роз'єм **USBA**, розташований на панелі Notebook і роз'єм **USBB**, розташований на задній панелі **ЦПК**;

• кабель **Мережа** підключається до мережі 220В 50 Гц;

Апаратура, що входить в комплекс, забезпечує виконання наступних функцій:

• перетворювач радіочастот (ПРЧ) забезпечує прийом сигналів у діапазоні частот 0.01 – 3000 МГц і перетворює їх в другу проміжну частоту 10.7 МГц з смугою пропускання не менше 4МГц. Крім того ПРЧ забезпечує детектування сигналів, що приймаються для прослуховування.

• блок АЦСП з БПО синтезує частоти в смузі 4 МГц з кроком 20 кГц і перетворює сигнал з другої ПЧ в квадратурний форму забезпечує швидкість сканування 200 Мгц / сек, тим самим забезпечуючи перегляд робочого діапазону вимірювача (з урахуванням часу перемикання БПРЧ через 4 МГц) зі швидкістю 80МГц/сек в діапазоні частот 30 ... 3000 Мгц. У діапазонах частот 0.01 ... 12.5 МГц та 12.5 ... 44 МГц крок перебудови 30 і 200 кГц відповідно.

Даний блок забезпечує також третє перетворення частоти в «Нульову», фільтрацію сигналу і формування двох квадратурних каналів і забезпечує обчислення двох функцій взаємної кореляції X і Y між прийнятими коливаннями $U_c(t)$ і формованими блоком косинусоїдальним $U_0(t)\cos\varpi_0 t$ і синусоїдальним $U_0(t)\sin\varpi_0 t$ сигналами, тобто:

$$X = U_c U_0(t)\cos\varpi_0 t; \qquad (1)$$
$$X = U_c U_0(t)\sin\varpi_0 t.$$

• Блок АЦСП проводить фільтрацію і перетворення аналогових сигналів, що надходять по двох каналах **X** і **Y**, в цифрову форму з тактовою частотою 156 кГц і керує всіма пристроями вбудованими в ЦБК. Дані сигнали виводяться у вікні Аналізатор /

• Персональний комп'ютер виконує наступні функції:

а) обробляє оцифровані сигнали X і Y, зводить їх в квадрат, підсумовує і обчислює квадратний корінь.

$$\sqrt{U_c^2(t)U_0^2(t)\left[\cos^2\varpi_0 t + \sin^2\varpi_0 t\right]} = \qquad (2)$$
$$= U_c U_0(t) = Z(t).$$

З формули (2) видно, що значення кореляційної функції Z(t) не залежить від початкової фази сигналу і при нормуванні $U_0(t) = 1$ дорівнює його амплітуді, тобто:

$$Z(t) = U_c(t). \qquad (3)$$

Таким чином у вимірювачі реалізований оптимальний пристрій виявлення, який є лінійним пристроєм, що дозволяє проводити вимірювання амплітуд безперервних і імпульсних сигналів і шумів. Значення амплітуди Z(t) виводиться у вікні програми Аналіз / Амплітуда в Головному вікні програми, вигляд якої наведено на рис. 2;

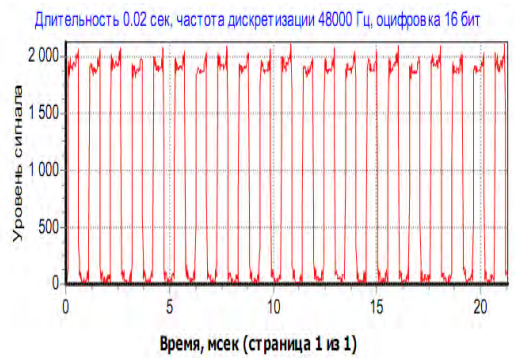

Рис. 2. Вид вхідного сигналу у вікні Амплітуда

б) керує апаратурою вимірювача, обробляє сигнали за допомогою спеціального програмного та математичного забезпечення, проводить розрахунок вимірювальних параметрів сигналів, приймає логічні рішення при роботі вимірювача в автоматичному режимі, відображає сигнальну та іншу інформацію, протоколює отримані результати.

• Блок БВЧК являє собою швидкодіючий широкосмуговий ВЧ-коммутатор, який можна підключити до вимірювача додаткових антен для виявлення сигналів. У вимірювальному тракті вимірювач використовується антенний вхід ANT 2.4 блоку для підключення внутрішнього калібратора.

• Блок живлення здійснює перетворення напруги 220В в стабілізоване 12В, яке забезпечує живлення основного блоку вимірювача.

• Акумуляторная батарея ємністю 2А/год забезпечує автономне живлення вимірювача протягом однієї години.

• Виміпювання сигналів проводиться в автоматичному режимі за списком частот або на фіксованій частоті по команді оператора. При виборі режимів вимірювання потрібно керуватися наступним:

– для імпульсних і амплітудно-модульованних сигналів використовуються режими виміру «P», «SA», «S», максимальна амплітуда, усереднена амплітуда, середнє значення, ефективне і амплітудне значення;

– для немодульованих сигналів використовуються режими «F», «A»;

– для вимірювання шумів використовується режим середньоквадратичне значення;

– для імпульсних сигналів використовується режим «Квазіпікове значення» за ГОСТ 11001-80.

Режим Максимальна амплітуда використовується для вимірювання максимального значення з імпульсної послідовності сигналів, зображеної на рис. 3.

Режим Усереднення амплітуди використовується для вимірювання середньої амплітуди з імпульсної послідовності сигналів (рис. 3):

$$U_{mk} = \frac{\sum_{i=1}^{n} U_i}{n}, \quad (4)$$

де n – кількість імпульсів в аналізованій послідовності; U_i – поточні значення амплітуд імпульсів.

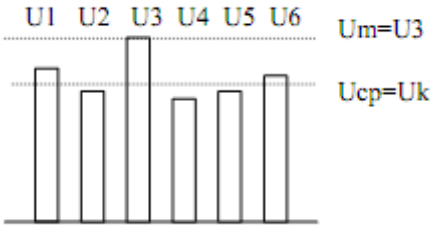

Рис. 3. Імпульсна послідовність сигналів

Середньоквадратична помилка визначається за формулою:

$$\delta_{Umk} = \frac{\sum (U_{mk} - U_i)^2}{n-1}. \quad (5)$$

Середньоквадратичний рівень шумів (режим «SK») визначається за формулою

$$U_{ck} = \left[\frac{1}{T} \int_0^T U_x^{\ 2}(t)dt \right]^{\frac{1}{2}}, \quad (6)$$

де T – інтервал вимірювання режимів; $U_x(t)$ – значення рівня шумів на інтервалі вимірювання.

Середнє значення (режим «S») визначається за формулою

$$U_{cp} = \frac{1}{T} \int_0^T U_x(t)dt. \quad (7)$$

Включається цифровий вимірювач, який видає відповідне виміряне значення сигналу Uo.

За допомогою комплексу АКОР-2ПК проведено дослідження тактових частот та рівнів сигналу на можливість зняття інформації за рахунок ПЕМВН.

Дослідження проводились у Львівському регіональному центрі технічного захисту інформації з використанням вимірювальних антен:

– АИ5-0 для вимірювання електричної складової поля;

– АИР3-2 для вимірювання магнітної складової поля;

– ТИ2-3 струмознімача для вимірювання наведень в колах живлення.

Також було використано подовжувач USB типу Firewire 4/ 4 FWP-44-10 для отримання більш чіткого сигналу.

Дослідження проводимо на ПЕОМ склад якої наведено у табл. 2.

Дослідження проводилось з застосуванням методу примусової активізації, який полягає у активізації каналу еталонним сигналом, що дозволяє ідентифікувати випромінювання, і виміряти рівні що виникають в результаті ПЕМВН.

Результати вимірювань ПЕМВН флеш носіїв приведені в табл. 3.

Таблиця 2

Склад ПЕОМ

Тип комп'ютера	Однопроцессорный комп`ютер с ACPI
Операційна система	Microsoft Windows XP Professional
Пакет обновлення ОС	Service Pack 3
Чіпсет системної плати	Intel Lakeport-G i945GC
Системна пам'ять	503 Мб (DDR2-667 DDR2 SDRAM)
Контролер USB1	Intel 82801GB ICH7 - USB Universal Host Controller [A-1]
Контролер USB2	Intel 82801GB ICH7 - Enhanced USB2 Controller [A-1]
USB-пристрій	Запом'ятовучий пристрій для USB

Таблиця 3

Результати вимірювання
та порівняльні характеристики флеш носіїв

Фірма виробник	Pretec	Transcend	Kingston	Transcend	PQI
1	2	3	4	5	6
Модель	Wave	JetFlash V30	Data Traveler 102	Rectractable	U 273
Об'єм пам'яті (Gb)	1	2	4	8	16
Визначення тактової частоти програмно-математичним методом:					
Тактова частота (MHz)	19,00	22,007	15,64	21,61	10,45
Обмірюваний рівень сигналу, мкВ/м	31,4	54,5	48,2	32,1	39,1
Обмірюваний рівень сигналу, Дб/мкВ/м	29,9	34,6	33,7	30,1	31,8
Тактова частота (MHz)	37,98	44,26	31,37	43,20	20,98
Обмірюваний рівень сигналу, мкВ/м	48,2	45,5	39,1	29,0	24,2
Обмірюваний рівень сигналу, Дб/мкВ/м	33,7	33,2	31,8	29,2	27,7
Тактова частота (MHz)	57,02	66.29	46,96	64,84	31,35
Обмірюваний рівень сигналу, мкВ/м	39,1	59,8	32,5	33,8	31,3

1	2	3	4	5	6
Обмірюваний рівень сигналу, Дб/мкВ/м	31,8	35,7	30,2	30,6	29,9
Тактова частота (MHz)	75,976	88,063	–	–	–
Обмірюваний рівень сигналу, мкВ/м	28,9	40,1	–	–	–
Обмірюваний рівень сигналу, Дб/мкВ/м	29,2	31,2	–	–	–
Визначення тактової частоти та рівнів сигналу магнітної складової за допомогою АКОР-2ПК:					
Тактова частота (MHz)	19,00	22.00	15,64	21,61	10,45
Обмірюваний рівень сигналу, мкВ/м	49,8	52,8	51,9	31,4	59,5
Обмірюваний рівень сигналу, Дб/мкВ/м	33,9	34,5	34,3	29,9	35,5

Узагальнюючи результати вимірювань, які приведені в табл. 3 можна сказати таке:

- USB порт розрізняє тип USB від USB1 автоматично, тому тактові частоти будуть залежати від параметрів тракту USB для кожної ПЕОМ;
- тактова частота в ефірі вища від розрахованої тестом. Очевидно, розробники тестів використовують коефіцієнти, отримані на окремій ПЕОМ для окремого випадку;
- миттєва частота вища за розраховану середню;
- амплітуди сигналів значно відрізняються в залежності від типу корпусу флеш носія. Металеві корпуси практично повністю екранують сигнал. Металеві корпуси флеш-носіїв дозволяють виявити ПЕМВН від флеш за 0,1 метра.
- застосування екранованого USB продовжувача типу Firewire зумовлене випромінюванням від тракту USB материнської плати ПЕОМ. При наявності в ПЕОМ інших USB приладів відбувається додаткове маскування тест-сигналу від флеш носіїв.

Список літератури

1. Закон України «Про інформацію». – К.: ВР України, 1992. – 15 с.

2. Зибін С.В. Автореферат дисертація. Оцінка захищеності об'єктів автоматизованої системи керування повітряним рухом з урахуванням несанкціонованого доступу / С.В. Зибін. – К., 2006. – 18 с.(ДСК).

3. ТР ЕОТ-95. «Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок». – К.: ДСТЗІ України, 1995. – 10 с.

4. Бузов Г.А. Защита от утечки информации по техническим каналам / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. – М.: Горячая Линия – Телеком, 2005. – 416 с.

5. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – К.: Юниор, 2003. – 504 с.

6. Скляров Д.В. Мистецтво захисту й злому інформації / Д.В. Скляров. – СПб.: БХВ-Петербург, 2004. – 271 с.

7. Торокин А.А.. Инженерно-техническая защита информации / А.А. Торокин. – М.: Гелиос АРВ, 2005. – 306 с.

8. Домарев В.В. Защита информации и безопасность компьютерных систем / В.В. Домарев. – М.: Диа-Софт, 2001. – 299 с.

9. Конахович Г.Ф. Защита информации / Г.Ф. Конахович. – М.: МК-Пресс, 2005. – 281 с.

10. Ананский Е.В. Защита информации – основа безопасности бизнеса [Єлектронний ресурс] / Е.В. Ананский. – 2005. – Режим доступу до ресурсу: http://www.bezpeka.com.

Надійшла до редколегії 15.04.2011

Рецензент: д-р техн. наук, проф. О.О. Кузнецов, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

ИССЛЕДОВАНИЕ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ ОТ ФЛЕШ НОСИТЕЛЕЙ

В.Б .Дудыкевич, И.С. Собчук, Л.М. Ракобовчук, В.С. Зачепыло

В данной работе сделан обзор проблем возникновения электромагнитного излучения от средств електроно - вычислительной техники. Проведен анализ информации, которая обрабатывается с помощью средств електроно вычислительной техники. Особое внимание уделено анализу и описанию технических каналов истока информации, выбору имеющихся средств защиты информации. В работе описан принцип работы и методика измерения побочного электромагнитного излучения с помощью автоматизированного комплекса АКОР-2ПК. В завершающей части проведено исследование и сравнительная характеристика измерения электромагнитного излучения от флеш носителей с помощью АКОР-2ПК.

Ключевые слова: *побочные электромагнитные излучения и наводи, ПЭМВН.*

INVESTIGATION OF SIDE ELECTROMAGNETIC RADIATION FROM FLASH MEDIA

V.B. Dudykevich, I.S. Sobchuk, L.M. Rakobovchuk, V.S. Zachepilo

In this work review of problems of electromagnetic radiation from facilities of electronic computing engineering is realized. There was done analysis of information which is processed by facilities electronic computing engineering. Considerable attention is spared to the analysis and description of the technical ductings of information source, choice of present priv facilities. In this work principle of work and measuring method of side electromagnetic radiation by the automated complex AKOR-2PK are described. In finishing part there are researched and done comparative description of electromagnetic measuring of radiation from flash memory by AKOR-2PK.

Keywords: *adverse electromagnetic radiation and directs, PEMVN.*