УДК 004.056.53 **Луценко В.М., Якименко О.М.(НТУУ «КПІ»)**

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ЛОКАЛЬНИХ ДЖЕРЕЛ ПОБІЧНИХ ВИПРОМІНЮВАНЬ ПЕРСОНАЛЬНИХ КОМП'ЮТЕРІВ ПРИ СТВОРЕННІ КСЗІ

Розглянуто проблему щодо перегляду підходів до захисту інформації від витоку каналами побічних електромагнітних випромінювань за рахунок екранування в окремих комп'ютерах у складі об'єктів технічних засобів перетворення інформації, автоматизованих системах або виділених приміщеннях при використанні комп'ютерів у якості технічних засобів перетворення інформації. Зазначається, що така проблема є особливо важливою при реалізації комплексної системи захисту інформації.

Вступ. Наразі при створенні комплексних систем захисту інформації (КСЗІ) [1] автоматизованих систем (АС), окремих персональних комп'ютерів (ПК) у складі об'єктів технічних засобів перетворення інформації (ТЗПІ) або у виділених приміщеннях при використанні ПК у якості ТЗПІ, задача захищеності об'єкту вимагає залучення методів та засобів визначення ступеню об'єктивної стійкості ПК від інформаційних атак. Так, наприклад, при розгляді етапів створення КСЗІ згідно [2] п. 6.2.1 «Вивчення об'єкта у вигляді НДР» виконання робіт для зазначених видів об'єктів вимагає проведення робіт з визначення можливих загроз від ПК, котрі передбачається використовувати, а при відсутності ПК у захищеному виконанні або додатково дороблених до необхідного рівня захищеності, вимагає і значних ресурсів і, загалом, не є завданням, притаманним розробникам КСЗІ таких об'єктів. З іншого боку, з появою нових технічних рішень в галузі створення ПК загального користування з'явилася необхідність перегляду підходів щодо захисту інформації від витоку каналами побічних електромагнітних випромінювань (ПЕМВ). Таке завдання є актуальним ще з часів Г. Ядлі, що розробляв способи виявлення та перехоплення прихованих радіопередач для армії США. При проведенні дослідження Ядлі звернув увагу на наявність побічних випромінювань та припустив, що вони також можуть нести корисну інформацію [3].

Питання пошуку та вимірювань ПЕМВ ПК залишається гострим. Дослідження можливості перехоплення інформації, що обробляється ПК, цікавить наразі не тільки державні установи та служби безпеки, а також і власників підприємств та приватних користувачів. Технології ПК постійно розвиваються, тому боротьба з їх ПЕМВ триває постійно і з часом змінюються підходи до розв'язання даної проблеми. Один з таких підходів є предметом розгляду у даній статті.

Питання щодо методики спеціальних досліджень ПЕМВ ПК. Методи захисту ПК поділяються на активні та пасивні. Пасивні методи є основними методами захисту, а активні використовуються тоді, коли необхідною є підтримка пасивних. Найбільш поширеними пасивними методами є [4]:

1. Використання автономних або стабілізованих джерел електроживлення ТЗПІ;
2. Використання в колах електроживлення ТЗПІ, а також в лініях освітлювальної та розеткової мережі в межах контрольованої зони та виділених приміщень, протизавадних фільтрів;
3. Заземлення ТЗПІ та екранів з'єднувальних ліній;
4. Екранування ТЗПІ та з'єднувальних ліній.

Наведені методи можуть використовуватися як поодинці так і в комплексі але заземлення має бути обов'язково.

Зазвичай реалізація екранування ТЗПІ відбувається шляхом повного закриття ПК в екрануючий кожух. Вартість такої спецтехніки складає десятки тисяч гривень і, загалом, не створює передумов для гарантованого отримання характеристик визначеного заздалегідь технічним завданням ступеня захисту. Тому виникає потреба в нових методах захисту які б значно знизили вартість засобів захисту, зменшили кошторис та термін робіт, створили умови для обгрунтованості застосування засобів захисту.

Для визначення методу захисту, нового для вітчизняних ПК у захищеному виконанні, котрий розглядається в рамках даної статті, необхідно проаналізувати механізми створення ПЕМВ в ПК на прикладі пристроїв формування інформації на екрані монітору.

Відтворення інформації на екрані монітору є найбільш небезпечною функцією роботи ПК з точки зору можливого утворення каналів витоку інформації [5]. У формуванні відеозображення на екрані бере участь відеопідсистема, котра складається з двох основних частин: відеоадаптера і монітора. Відеоадаптер призначений для формування відеосигналу. Перед тим як стати зображенням на моніторі цифрові дані про зображення опрацьовуються центральним процесором ПК. Дані з його оперативної пам'яті через шину даних потрапляють до процесора відеоадаптера, де вони обробляються та зберігаються в відеопам'яті. В відеопамяті створюється цифрове зображення, яке має бути відтвореним на екрані монітора. За тим, дані в цифровому форматі що містять образ зображення, передаються з відеопамяті до цифро-аналогового перетворювача, де перетворюються в аналоговий вигляд і тільки після цього потрапляють до монітора з електронно-променевою трубкою (ЕПТ). З появою рідкокристалічних (ЖК) дисплеїв потреба в цифро-аналоговому перетворенні сигналу зникає. Але цей елемент все одно присутній в відеокартах на випадок підключення аналогових моніторів через рознімач VGA.

Екран монітора відображає інформацію у вигляді крапок – пікселів. Усі разом пікселі утворюють цілісне зображення яке оновлюється від 50 до 120 раз на секунду в залежності від типу дисплея та даних, що надаються відеокартою. Монітори з ЕПТ оновлюють дисплей рядками, а плоскі ЖК монітори оновлюють кожний піксель як окремий елемент.

Теоретично, джерелами ПЕМВ на відеокарті можуть бути: перетворювальні ланцюги, область поблизу рознімача, пам'ять та процесор.

Для перевірки теоретичних припущень щодо визначення джерел ПЕМВ було проведено низку експериментів, один з результатів котрих наведений на рис.1.

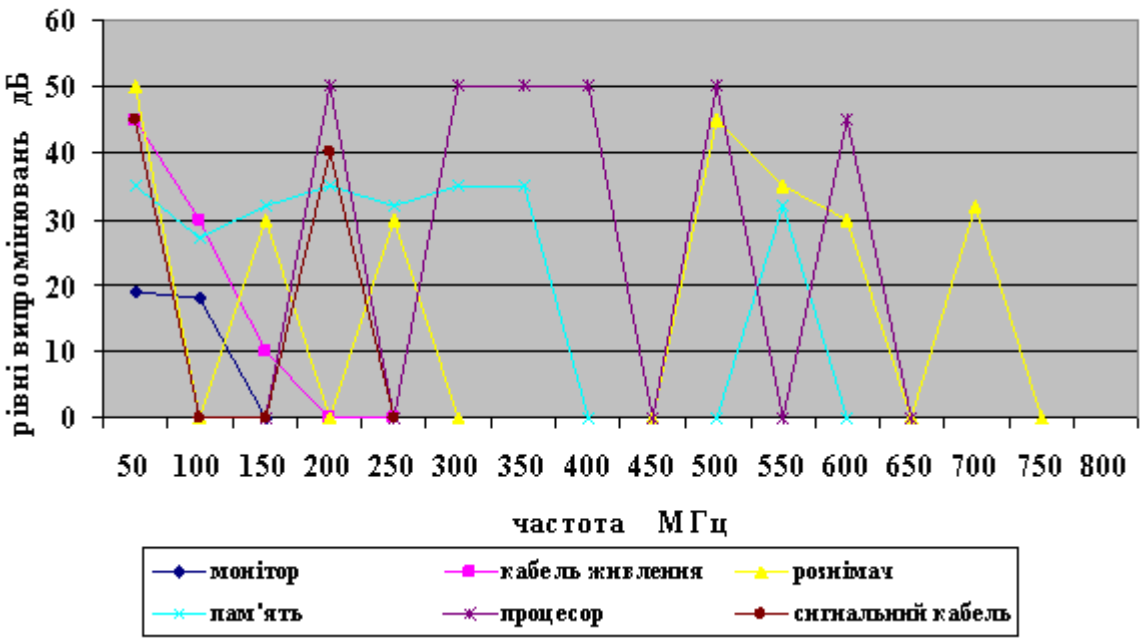

Рис.1 Графіки залежності рівня випромінювань від частоти для кожного елементу відеотракту

Для проведення даних досліджень була використаною окрема методика. Зміст методики полягає у тому, що вимірювання поділяються на 2 етапи: підготовчий етап та проведення безпосередніх вимірювань.

На першому етапі проводяться вимірювання рівнів ПЕМВ у відеотракті при роботі комп'ютера в тестовому для монітора режимі. Результати вимірювань формують у вигляді таблиці рівнів сигналів та частот на яких виявлений інформативний тестовий сигнал. В якості чутливого елемента приймача використовуються антени АИ 5-0 та АИР 3-2. В якості вимірювального блоку приймача використовуються селективні вольтметри, а саме: SMV-11 для діапазону частот до 30 МГц та SMV 8.5 для діапазону частот до 1 ГГц. Ознакою несучої частоти інформативного сигналу є наявність характерного звукового сигналу тесту. При вимірюваннях для кожної частоти зазначається тип антени, котра використовується. Загальна схема вимірювань наведена на рис.2. Складена таблиця дає змогу визначити частоти ПЕМВ, котрі характерні для даного відеотракту.

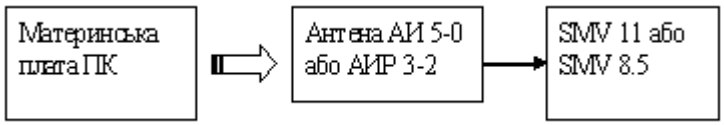

Рис. 2. Загальна схема вимірювань для першого етапу методики

Маючи список частот з відповідними рівнями сигналів, на наступному, другому, етапі можливим є визначення місцеположення елемента плати ПК з найбільш високим рівнем ПЕМВ на визначених частотах. При цьому ПК налаштовується в тестовий режим, як і на першому етапі. Вимірювальна апаратура налаштовується на одну з частот, котра визначена на попередньому етапі роботи як небезпечна, та відповідно занесена до таблиці. На відміну від першого етапу використовується спеціальна точкова антена, замість типових АИ 5-0 або АИР 3-2. За допомогою точкової антени визначаються відносні рівні сигналів поблизу окремих елементів плати по черзі. У даному випадку точне значення рівня сигналу не є потрібним, оскільки метою вимірювань є визначення компонентів плати з найбільшими за рівнем випромінюваннями у порівнянні з іншими компонентами плати. Змінюючи відстань до елемента системи та положення приймальної антени, можна знайти максимальне значення магнітної та електричної складової електромагнітного поля. Відстань змінюється від 0 до 2-3 см., а кут нахилу антени змінюється від 0^0 до 90^0.

Процедуру другого етапу повторюють для усіх частот згідно списку частот, отриманому на першому етапі.

За отримання відносних значень рівнів ПЕМВ від різних елементів системи ПК в результаті аналізу результатів вимірювань визначаються елементи та вузли найбільш небезпечні за потужністю випромінювань небезпечних сигналів. Отримуються дані не тільки щодо розташування таких елементів, а і щодо взаємних зв'язків між ними через електромагнітні поля, характеристик наведень випромінювань з небезпечними сигналами на трасовані провідники материнської плати, наявності взаємних зв'язків між провідниками, місць розташування концентраторів полів на вигинах трасованих провідників та на електронних компонентах, напрямків випромінювань, характерних місць утворення полів окремо за магнітною та електричною складовою. Згідно отриманих даних визначаються способи доробки ПК до стану з визначеною зоною розвіддосяжності.

Висновки. Викладена методика виявлення елементів персонального комп'ютера в якості джерел ПЕМВ, дає можливість індивідуального підходу до кожного елемента системи та розробки відповідних методів його захисту. Підґрунтям для такого підходу є результати вимірювань, проведених авторами даної роботи. Очевидно, що для локалізації випромінювань поблизу їх джерел немає необхідності у використанні екранів для блоку ПК в цілому, адже місце елементів ПК, що випромінюють ПЕМВ, чітко визначається. Такі елементи створюють випромінювання в відповідних частотних діапазонах. Так, за результатами експериментів виділено три небезпечні місця відеокарти: процесор, пам'ять та область рознімача, а екран монітора має відносно незначні ПЕМВ. Визначені як найбільш

небезпечні джерела ПЕМВ можуть бути захищені шляхом створення окремих екрануючих конструктивів. До переваг такого підходу можна віднести:

– можливість використання більш технологічного підходу для забезпечення захищеності ПК ще на етапі типової процедури збирання материнської плати, без застосування окремих громіздких конструктивів спеціального призначення, а саме: екранування плати в цілому, екранування системного блоку в цілому, застосування спеціального трасування провідників, проектування захисних фільтрів для живлення окремих вузлів ПК, спеціальне проектування схемної «землі», та ін.;

– спрощена процедура доведення вже вироблених ПК до захищеного виконання при використанні такого ПК в інтересах проектування КСЗІ конкретних об'єктів;

– зменшення металоємності конструкції плати, що призводить до зменшення вірогідності появи випадкових антен у вигляді додаткових металевих екранів великого розміру, при наявності реактивної компоненти у зв'язках «екран-земля», а також підвищення вірогідності виходу діапазону частот випромінювань за межі нормованого діапазону, де екрануючі конструкції можуть отримувати якості приймально-передавальних випадкових антен;

– забезпечення менш напруженого теплового режиму роботи елементів ПК за рахунок безперешкодного доступу повітря до них;

– зменшення вартості створення ПК у захищеному виконанні;

– об'єктивність використання захисних засобів за рахунок цільового та індивідуального втручання у конструктиви вузлів та розташування електронних компонентів ПК.

За результатами досліджень виявлені випадки, котрі визначають можливість схемних рішень що дозволяють отримати ефект згладжування крутизни фронтів імпульсів ПЕМВ. При цьому зменшується потужність їх випромінювань.

Загалом, зазначений підхід є раціональним і таким, що дозволяє у багатьох випадках спрощувати процедуру проектування систем захисту інформації для автоматизованих систем. Наприклад, більш визначеним і предметно спрямованим стає завдання щодо складання технічного проекту на 5 етапі проектування автоматизованих систем згідно [6]. Крім того, при побудові систем захисту інформації згідно [1] на етапах «визначення й аналізу загроз» та «розроблення системи захисту інформації» процедура проектування для об'єктів АС ЗОТ спрощується, оскільки заздалегідь є відомими можливості ПК щодо створення каналів витоку за рахунок ПЕМВ. На етапі створення КСЗІ в інформаційно-телекомунікаційних системах згідно п.6.1.2.9 [2] «Визначення переліку об'єктів захисту, перелік загроз, модель загроз, модель порушника» та на етапі п.6.4.3 «технічний проект» спрощується завдання для проектувальника КСЗІ, оскільки більш визначеним є питання використання ПК у захищеному виконанні або додаткове доведення ПК до вимог захищеності.

Література

1. ДСТУ 3396.0-96 «Технічний захист інформації. Основні положення».

2. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

3. О.В. Мотуз «Побочные электромагнитные излучения: моменты истории.// Защита информации. Конфидент. 2001.№1. С86…89.

4. Хорев А.А. Способы и средства зашиты информации. - М.: МО РФ, 2000. - 316 с.

5. А. А. Хорев "Оценка эффективности защиты средств вычислительной техники от утечки информации по техническим каналам", "Специальная техника", №4 (2007).

6. ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания».

Надійшла: 02.06.2011 р.

Рецензент: д.т.н., проф. Дудикевич В.Б.