УДК 004.9

Б.Д. Будз
Національний університет «Львівська політехніка»
кафедра «Захист інформації»
79000, м. Львів, вул. Кн.Романа, 3

ОРГАНІЗАЦІЙНІ ПІДХОДИ ДО ПРОТИДІЙ ВИТОКУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ КАНАЛАМИ ПЕМВ

The article studies organizational methods of preventing confidentional information leakage through technical channels. The study demonstrates the research results of compromising emanations of graphics cards of one type in different graphic modes. The research shows that graphic cards of one type differ in compromising emanations parameters. According to the study results, compromising emanations of a graphic card depend on the mode types. The research results may be used in PC hardware configuration to process the limited access information as well as organizing complex information security systems.

Keywords – compromising emanations, technical channel of information leakage, graphics card, security zone of information, organising the event, processing the limited access information, safe PC, information leakage.

У статті розглянуто організаційні методи для протидії витоку конфіденційної інформації технічними каналами. Наведені результати досліджень значень ПЕМВ відеоадаптерів одного сімейства в різних режимах роботи. Показано, що відеоадаптери одного сімейства мають розкид параметрів ПЕМВ. Також продемонстровано що розкид параметрів одного відеоадаптера залежить від режимів роботи. Результати досліджень можна використовувати при конфігуруванні ПК для оброблення ІОД, а також при побудові КСЗІ.

Ключові слова – ПЕМВ, ТКВІ, відеоадаптер, контрольована зона, організаційний захід, обробка ІОД, захищений комп'ютер, витік інформації.

Актуальність. Сучасні тенденції ведення господарської діяльності в державних і приватних установах переконливо свідчать, що основним засобом, який забезпечуватиме зберігання, оброблення і передавання інформації яка утворюється в процесі функціонування цих установ буде комп'ютер, який ми звикли називати персональним (ПК) або автоматизованою системою (АС). За своїм характером інформація може бути відкритою або з обмеженим доступом (ІОД). Інформація відкритого характеру не потребує захисту від витоку, оскільки не несе відомостей, які можуть бути цікавими з точки зору розвідки. ІОД можна розділити на дві категорії: ІОД яка є власністю держави, і та інформація, яка є критичною для установи, оскільки її витік може призвести до завдання економічних збитків, зокрема банкрутства.

Що стосується ІОД яка є власністю держави, то питання протидії її витоку регламентуються відповідними нормативними актами, які затверджені державними органами, які відповідають за реалізацію державної політики у сфері захисту державних інформаційних ресурсів, і вона чітко категорійована ("таємно", "цілком таємно", "особливої важливості"). Захист ІОД яка не є власністю держави але є критичною для установи, яку часто відносять до грифу "комерційна таємниця", лягає на плечі керівництва установи.

На цей час відомо три підходи до протидії витоку ІОД через канал ПЕМВ з ПК: технічний, організаційний і організаційно-технічний. В більшості спеціалізованих видань і інтернет ресурсах,

які висвітлюють питання захисті ІОД від витоку каналами ПЕМВН, наголос робиться на використання технічних заходів, таких як електромагнітне зашумлення, екранування засобів і приміщень, використання атестованих АС, тощо. Але проведення технічних мірoприємств для захисту ІОД потребує виділення значних коштів, які переважно відсутні, або недостатні на цей час. Якщо підходити до концепції захисту, то найкращим є варіант, коли захист забезпечується без фінансових витрат. Реалізувати такий захист можливо організаційними методами.

До організаційних методів для протидії витоку ІОД через канал ПЕМВ з ПК можна віднести:

- встановлення або розширення контрольованої зони (КЗ), яка поглинатиме зону R2;
- перенесення ПК в глибину КЗ;
- робота ПК в режимах, при яких зона R2 розміщена в межах КЗ;
- конфігурування ПК з апаратних засобів, які мають найменші значення зони R2, тощо;

Мета і задачі дослідження. Метою роботи є дослідження впливу серійності і конфігурації апаратних засобів ПК на значення рівнів ПЕМВ. На основі проведеного аналізу запропонувати підходи для протидії витоку ІОД під час обробки на ПК.

Опис лабораторної установки. Лабораторна установка, яка використовувалась для аналізу ПЕМВ, складалась з селективного мікровольтметра SMV-8, дипольних антен DP1 і DP3, осцилографа С-107, та використовувалась спеціальна програма, яка забезпечувала тестовий режим роботи апаратного засобу. Структурна схема лабораторної установки зображена на рис. 1. Для досліджень був обраний відеотракт ПК. Частотний діапазон SMV-8 – 30÷1000 МГц.

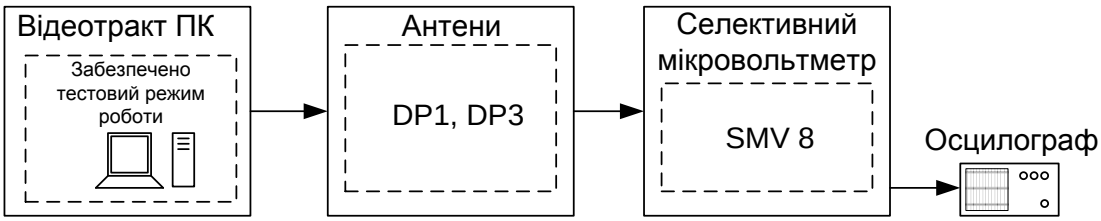
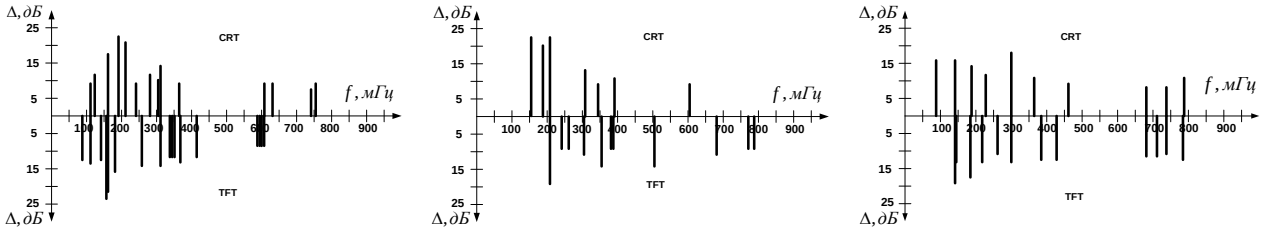


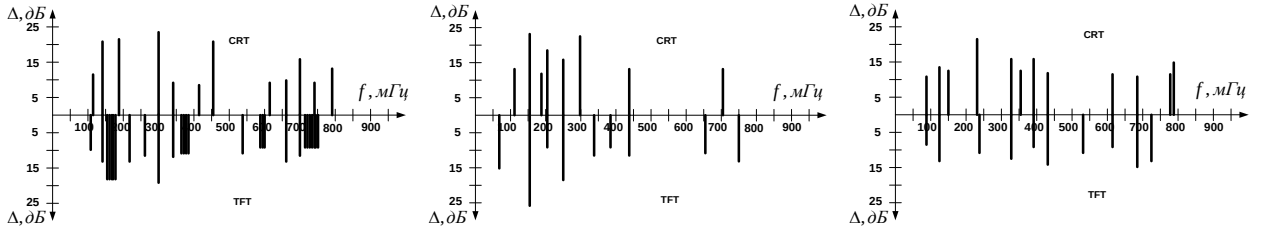
Рис. 1. Структурна схема лабораторної установки для дослідження ПЕМВ відеотракту ПК

Дослідження №1. Конфігурація відеотракту: відеокарта Nvidia Vanta/VantaLT 16 Мб, монітор CRT Samsung Samatron 55E з діагоналлю 17 дюймів, монітор TFT Daewoo HL720S з діагоналлю 17 дюймів. Результати досліджень наведені на рис. 2 - рис. 4.



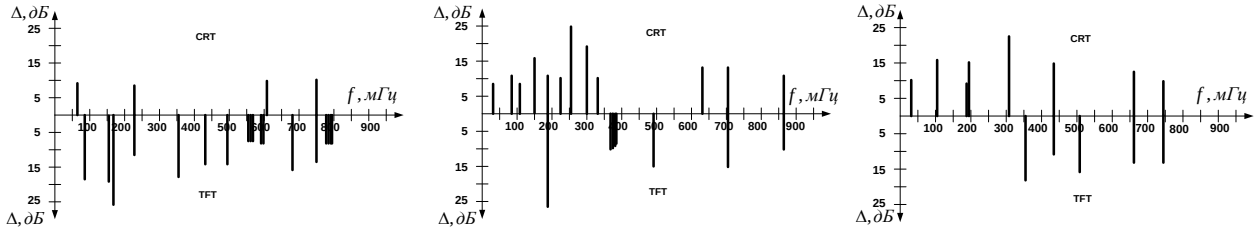
а) *б)* *в)*

Рис. 2. Значення рівнів ПЕМВ для CRT і TFT монітору при роздільній здатності 640×480 і частоті оновлення екрану 60 Гц - а), 70 Гц – б) і 72 Гц – в)



а) *б)* *в)*

Рис. 3. Значення рівнів ПЕМВ для CRT і TFT монітору при роздільній здатності 800×600 і частоті оновлення екрану 60 Гц - а), 70 Гц – б) і 72 Гц – в)



а) *б)* *в)*

Рис. 4. Значення рівнів ПЕМВ для CRT і TFT монітору при роздільній здатності 1024×768 і частоті оновлення екрану 60 Гц - а), 70 Гц – б) і 72 Гц – в)

Як видно з рисунків, зміна режиму роботи відеоадаптера ПК, до складу якого входить як CRT так і TFT монітор, призводить до зміни розкиду параметрів ПЕМВ. Слід зазначити що ні рівні випромінювання сигналу ні кількість частот випромінювань не свідчить про захищеність відеотракту від витоку через канал ПЕМВ. Для оцінки захищеності необхідно розрахувати зону R2 для кожного випадку, і лише отримавши значення величини зони R2 можна визначити той режим, який забезпечить найкращі характеристики з точки зору протидії витоку ІОД каналами ПЕМВ.

Дослідження №2. Конфігурація відеотракту: відеокарта Nvidia GeForce 210 512 Мб, монітор TFT Daewoo HL720S з діагоналлю 17 дюймів. Досліджено 8 відеоадаптерів однієї марки з однієї серії, при роздільній здатності 1024×768 і частоті оновлення екрану 60 і 75 Гц. Результати досліджень наведені на рис. 5 - рис. 6.

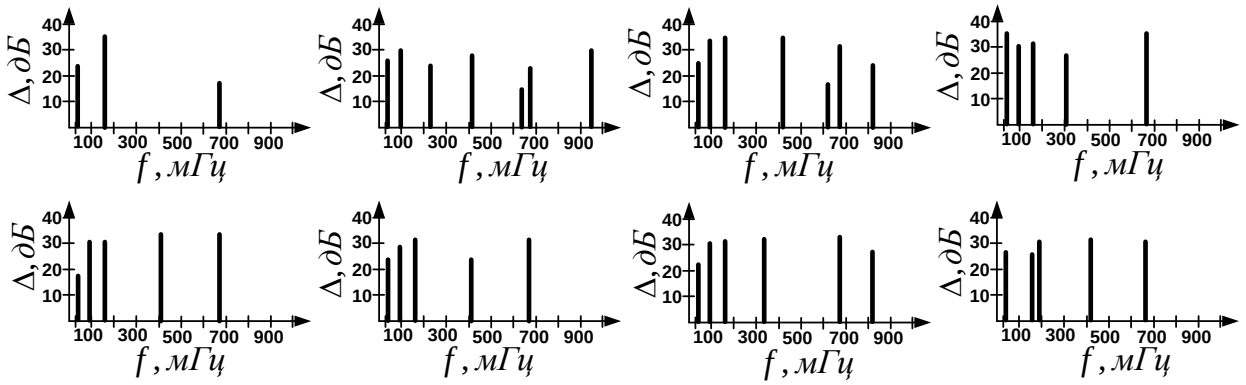


Рис. 5. Значення рівнів ПЕМВ 8 відеокарт Nvidia GeForce 210 512 Мб при роздільній здатності 1024×768 і частоті оновлення екрану 60 Гц

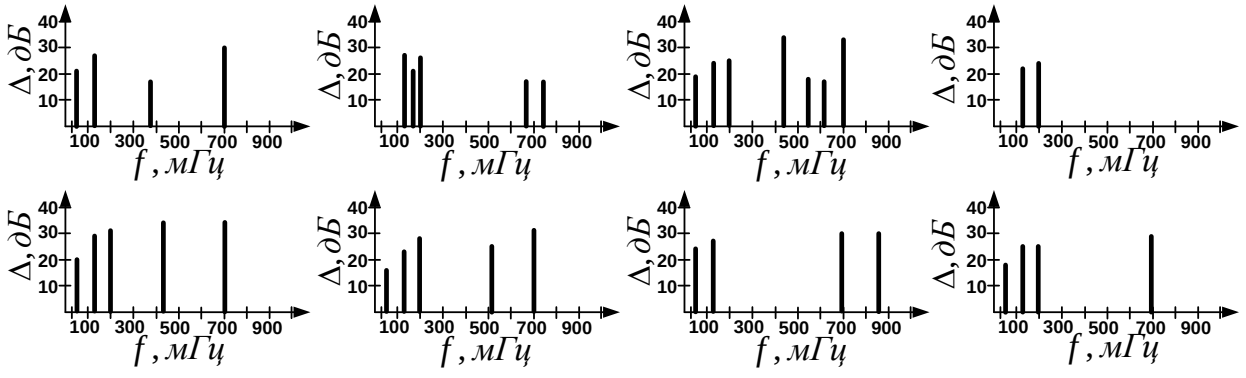


Рис. 6. Значення рівнів ПЕМВ 8 відеокарт Nvidia GeForce 210 512 Мб при роздільній здатності 1024×768 і частоті оновлення екрану 75 Гц

Як видно з рисунків за результатами досліджень, характеристики ПЕМВ кожного відеоадаптера є унікальні. Отже можна зробити висновок, що серед певної кількості однотипних апаратних засобів (в нашому випадку відеоадаптерів) однієї серії, можна виділити такі які мають

найменше значення зони R2. Тому при конфігурації ПК для подальшої обробки ІОД доцільно, при можливості, виявити ті апаратні засоби, які матимуть найменше значення зони R2. З наведених результатів також видно що зміна режиму роботи впливає на розкид параметрів ПЕМВ.

Дослідження №3. Конфігурація відеотракту: відеокарта Nvidia Vanta/VantaLT 16 Мб, монітор CRT Samsung Samatron 55E з діагоналлю 17 дюймів, монітор TFT Daewoo HL720S з діагоналлю 17 дюймів. Результати досліджень наведені на рис. 7 - рис. 8.

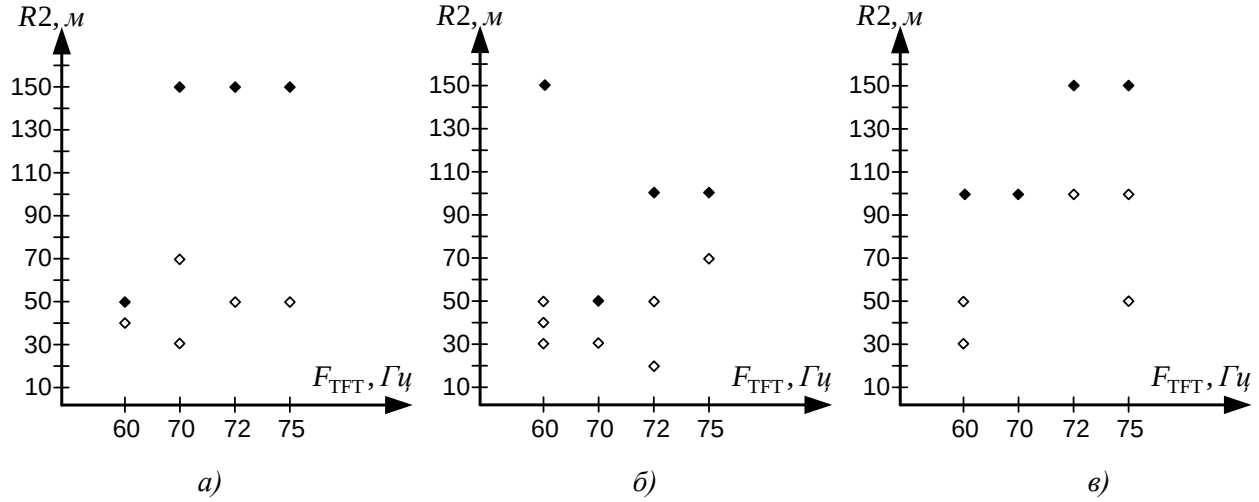


Рис. 7. Радіус зони R2 для відеотракту з TFT монітором при роздільній здатності 800×600 – а), 1024×768 – б) і 1152×864 – в) пікселів та частоті оновлення монітору 60, 70, 72 і 75 Гц.

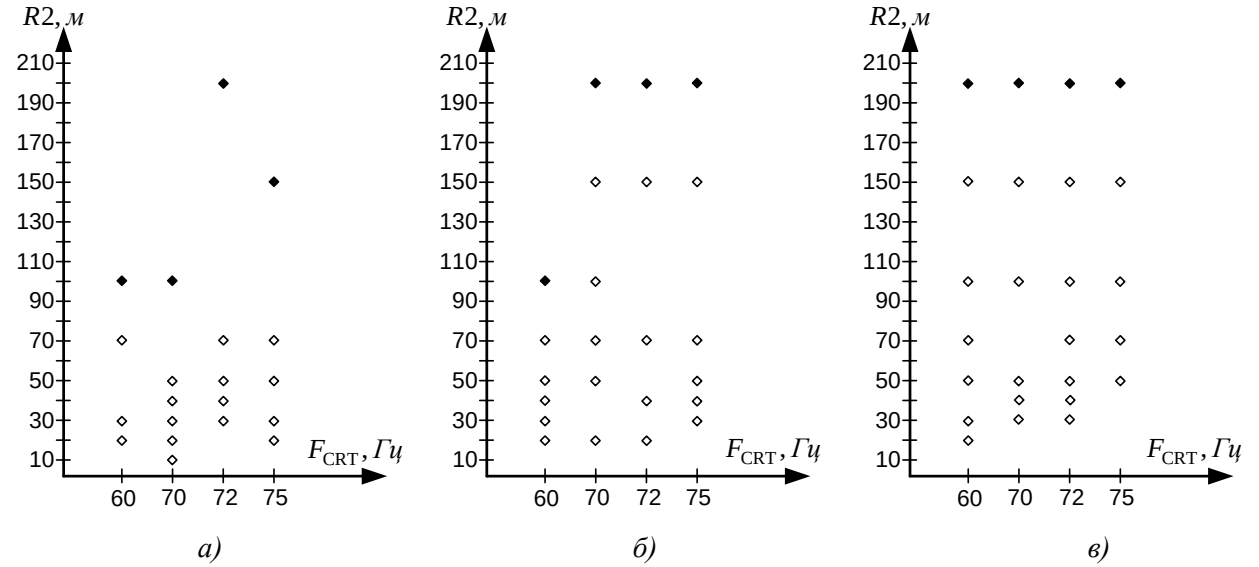


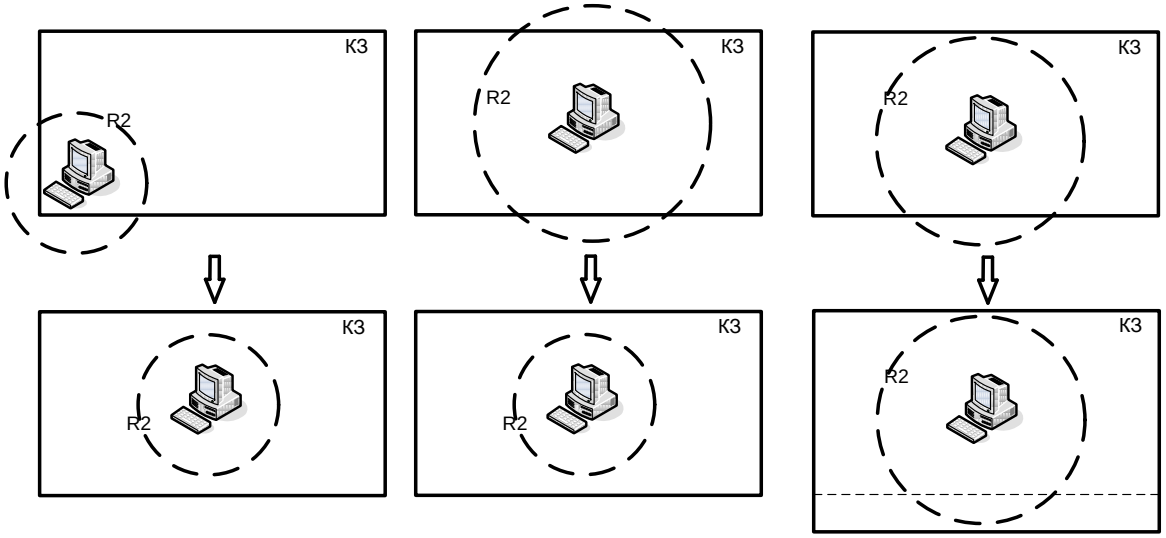
Рис. 8. Радіус зони R2 для відеотракту з CRT монітором при роздільній здатності 800×600 – а), 1024×768 – б) і 1152×864 – в) пікселів та частоті оновлення монітору 60, 70, 72 і 75 Гц.

Як видно з рис. 7, оптимальний режим роботи досліджуваного TFT монітору може бути при роздільних здатностях 800×600 і 1024×768 піксель та при частотах оновлення екрану 60 і 70 Гц відповідно. При таких конфігураціях величина зони R2 становить 50 метра, що в 3 рази менше за максимальну величину для цього типу монітора. З рис. 8 бачимо що оптимальний режим роботи досліджуваного CRT монітору може бути при роздільних здатностях 800×600 і 1024×768 піксель та при частотах оновлення екрану 60, 70 і 70 Гц відповідно. При таких конфігураціях величина зони R2 становить 100 метрів, що в 2 рази менше за максимальну величину для цього типу монітора. Отже зменшення величини зони R2 можна досягнути не використовуючи технічних засобів захисту, такі як екранування і електромагнітне зашумлення, достатньо "правильно" підібрати режими роботи відеоадаптера.

Проаналізувавши результати трьох експериментальних досліджень можна зробити наступні висновки:

- зміна режиму роботи відеотракту (роздільної здатності і частоти оновлення монітору) впливає на розкид параметрів ПЕМВ як для CRT так і для TFT моніторів;
- ПЕМВ характеристика відеокарт одного сімейства відрізняються, що дозволяє спеціалісту підібрати найоптимальніші, з точки зору захищеності, відеоадаптери для конфігурування ПК для обробки ІОД;
- завдяки програмним налаштуванням, можливо зменшити значення величини зони R2 в декілька разів, не використовуючи технічні засоби захисту.

На сьогодні можна виділити три найпоширеніших організаційних підходи для протидії витоку конфіденційної інформації через канал ПЕМВ, які зображені на рис. 9.



а) *б)* *в)*

Рис. 9. Варіанти організаційних підходів до протидії витоку ІОД каналами ПЕМВ, де КЗ – контрольована зона.

Перший метод (рис. 9 а) передбачає переміщення ПК в глибину КЗ так, щоб зона R2 ПК не виходила за межі КЗ. Як приклад, це може бути переміщення ПК з однієї кімнати в іншу. Другий метод (рис. 9 б) передбачає зменшення величини зони R2 до розмірів, при яких вина не виходитиме за межі КЗ. Цей випадок може виникнути тоді, коли нема можливості переміщати ПК, оскільки в будь-якому випадку зона R2 виходитиме за межі КЗ. Саме для цього випадку можна застосувати підходи, описані вище, а саме вибір оптимальної конфігурації апаратних засобів ПК. Третій метод (рис. 9 в) передбачає збільшення розмірів КЗ, якщо звичайно є така можливість. В деяких випадках з економічної точки зору цей підхід є більш ефективнішим ніж використання технічних засобів захисту.

Висновки. Конфігурація апаратних засобів ПК можна здійснювати програмно. Така зміна може вплинути на значення величини зони R2, що в свою чергу впливає на захищеність ПК який здійснює обробку ІОД. До складу ПК які передбачається використовувати для оброблення ІОД слід включати ті апаратні засоби, які мають найменше значення величини зони R2. Ці апаратні засоби можна вибрати з одного сімейства в магазині, або шляхом дослідження тих екземплярів які є на підприємстві. Використання організаційних підходів до протидії витоку ІОД через канал ПЕМВ дозволить зекономити кошти і забезпечити кращий захист інформації, на відміну від використання технічних методів захисту.

Список використаної літератури

1. Будз Б.Д., Дудикевич В.Б. "Приховані канали витоку інформації з використанням програмованих ПЕМВН", Науковий журнал Східноукраїнського національного університету імені Володимира Даля, № 2(4), 2010. 2. С. Колєсніков, Б. Будз "Дослідження і аналіз ПЕМВ відеоадаптера", Матеріали І-ої міжнародної науково-технічної конференції "Захист інформації і безпека інформаційних систем", с. 162-163, м. Львів.