

[DOI 10.28925/2663-4023.2026.34.1399](https://doi.org/10.28925/2663-4023.2026.34.1399)

УДК 621.396

Монахов Дмитро Вячеславович

аспірант

Київський столичний університет імені Бориса Грінченка, м. Київ, Україна

ORCID: 0009-0002-3471-4194

monakdim@ukr.net**Крючкова Лариса Петрівна**

доктор технічних наук, професор

професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Київський столичний університет імені Бориса Грінченка, м. Київ, Україна

ORCID: 0000-0002-8509-6659

l.kriuchkova@kubg.edu.ua

ІНФОРМАЦІЙНО РЕЛЕВАНТНІ ОЗНАКИ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ ПЕРСОНАЛЬНОГО КОМП'ЮТЕРА

Анотація. Функціонування будь-якого технічного засобу обробки інформації призводить до утворення ряду самочинних технічних каналів витоку інформації. Поширеними і небезпечними є канали, що спричиняються шляхом побічних електромагнітних випромінювань та наведень. Класична постановка задачі захисту інформації від витоку каналами побічних електромагнітних випромінювань та наведень переважно орієнтована на виявлення небезпечних випромінювань та визначення умов, за яких вони можуть бути використані для отримання інформації. Разом з тим актуальним є завдання виділення у множині побічних сигналів саме тих ознак, які мають стійкий зв'язок із конфіденційними даними та можуть бути перехоплені засобами технічної розвідки. Мета статті – дослідження інформаційно релевантних ознак побічних електромагнітних випромінювань складових персонального комп'ютера для вирішення завдань забезпечення захисту інформації на об'єктах інформаційної діяльності. В роботі досліджено побічні електромагнітні випромінювання персонального комп'ютера як технічний канал витоку інформації. Проаналізовано випромінювання відеотракту монітора, клавіатури та USB-інтерфейсу. Показано, що інформаційна значимість визначається не абсолютним рівнем випромінювання, а причинною залежністю від інформаційного вмісту, часовою та спектральною структурою, відтворюваністю, можливістю просторового або проводового поширення та стійкістю до завад. Для відеосигналу визначальними є компоненти, пов'язані з піксельною та кадровою розгортками й TMDS-символами; для клавіатури – часові переходи, матричне сканування та ознаки передавання кодів клавіш; для USB – залежні від даних диференціальні переходи та пакетна структура обміну. Запропоновано узагальнену послідовність відбору інформаційно релевантних ознак, що дає змогу встановлювати, в яких параметрах ПЕМВ може потенційно міститися конфіденційна інформація та за якими вимірювальними ознаками їх доцільно перевіряти.

Ключові слова: інформаційні технології; конфіденційна інформація; побічні електромагнітні випромінювання; технічний канал витоку; технічний захист інформації; відеосигнал; інформаційно релевантна ознака; електромагнітна сумісність.

ВСТУП

Широке застосування інформаційних технологій для передачі, приймання, обробки та зберігання інформації в різних сферах діяльності, з одного боку, сприяє підвищенню ефективності цієї діяльності, а з іншого – зумовлює виникнення загроз витоку інформації технічними каналами, під якими розуміється неконтрольоване поширення інформативного сигналу від його джерела через фізичне середовище до технічного засобу, який здійснює перехоплення інформації.

В переліку загроз важливе місце займають загрози витоку інформації каналами побічних електромагнітних випромінювань (ПЕМВ), а також внаслідок наведень інформативних сигналів в лініях



електроживлення технічних засобів обробки інформації, сполучних ліній допоміжних технічних засобів і систем, колах заземлення і сторонніх провідниках. Українська нормативна база технічного захисту інформації виділяє побічні електромагнітні випромінювання та наведення (ПЕМВН) як окремий технічний канал, що має враховуватися при організації захисту інформації з обмеженим доступом [1, 2]. У зарубіжній літературі використовуються терміни «compromising electromagnetic emanations» (компрометуючі електромагнітні випромінювання) [3] або TEMPEST (скорочення від «transient electromagnetic pulse emanation standard» – стандарт на електромагнітні імпульсні випромінювання, викликані перехідними процесами в електронній апаратурі) [3].

Проблема витоку конфіденційної інформації каналами побічних випромінювань інтенсивно досліджується з 1985 року, після першої відкритої наглядної демонстрації цього способу перехоплення інформації голландським інженером Вімом ван Ейком (Wim van Eck) [4]. Так, у 2004 році Маркус Кун (Markus Kuhn) здійснив перехоплення ван Ейка для ПК-моніторів [5]. Створено небезпечну технологію SoftTempest – технологію прихованої передачі даних по каналу побічних електромагнітних випромінювань за допомогою програмних засобів [6].

Дослідження проводяться за двома напрямками: вирішення задач, які виникають при перехопленні інформативних сигналів та вилученні з них конфіденційної інформації (задачі перехоплення); вирішення задач, які виникають при організації захисту конфіденційної інформації від витоку (задачі захисту). Сучасна електроніка дозволяє створювати мініатюрні і дуже чутливі приймачі. Використовується багатоканальний прийом сигналів з подальшою кореляційною обробкою, що дозволило суттєво збільшити дальність перехоплення інформації.

Класична постановка задачі захисту інформації від витоку каналами ПЕМВН переважно орієнтована на виявлення небезпечних випромінювань та визначення умов, за яких вони можуть бути використані для отримання інформації. Такий підхід є необхідним для практичної оцінки захищеності, однак залишає відкритим теоретичне питання формалізації виявлення наявності інформаційного вмісту у побічному електромагнітному сигналі, відокремивши його від фізичних, функціональних і випадкових складових. Наявність стійкої частоти, імпульсної компоненти або високого рівня електромагнітного випромінювання ще не означає, що зазначена ознака містить конфіденційну інформацію.

Мета статті – дослідження інформаційно релевантних ознак побічних електромагнітних випромінювань складових персонального комп'ютера (ПК) для вирішення завдань забезпечення захисту інформації на об'єктах інформаційної діяльності.

Постановка проблеми та принцип відбору інформаційно релевантних ознак ПЕМВ

У відкритій науковій літературі сформовано значний масив досліджень, у яких демонструється можливість відновлення або статистичного вилучення інформації шляхом перехоплення ПЕМВН. Дослідження охоплюють, зокрема, електромагнітні випромінювання дисплеїв, криптографічних пристроїв, клавіатур та інших електронних систем [7, 8]. Водночас ці результати здебільшого розв'язують конкретну задачу перехоплення або практичної атаки. Не вирішеним залишається питання побудови проміжної теоретичної моделі, що описує перехід від інформаційної змінної до набору спостережуваних ознак ПЕМВ та дозволяє встановити, які саме властивості побічного сигналу мають інформаційний вміст.

Для досягнення поставленої мети вирішувались такі завдання: 1) визначити багаторівневу модель виникнення інформаційного сліду; 2) формалізувати ознаки ПЕМВ як відображення конфіденційної інформації; 3) запропонувати критерій інформаційно релевантності ознаки; 4) дослідити ПЕМВ монітора, клавіатури та USB-інтерфейсу на предмет виявлення інформаційно релевантних ознак.

Електронні засоби опрацювання інформації функціонують завдяки змінним струмам, напругам і логічним переходам. Їхня фізична реалізація неминуче супроводжується утворенням електричних і магнітних полів, частина яких виходить за межі функціонального каналу передавання даних. В електромагнітній інформаційній безпеці такі побічні сигнали розглядаються як побічний фізичний канал, коли параметри вимірюваного поля або струму статистично чи детерміновано залежать від інформації, що обробляється пристроєм [1].

За фізичним шляхом поширення доцільно розрізняти просторовий канал, у якому інформаційно залежна складова поширюється у оточуючому просторі у вигляді електромагнітного випромінювання, та провідний канал, у якому вона передається по сигнальних, заземлювальних або силових провідниках. Обидва шляхи можуть існувати одночасно, а одна й та сама інформаційна подія може породжувати кілька спостережуваних проявів у різних частинах системи. Тому встановлення джерела ПЕМВ повинно завершуватися визначенням не тільки спектральної області, а й конкретного фізичного шляху її формування та поширення.

Інформаційно релевантною ознакою ПЕМВ доцільно вважати характеристику сигналу – часову, спектральну, кореляційну, просторову або комбіновану, зміна якої закономірно залежить від інформаційної події та яку можна стабільно виділити на тлі завад. Важливо, що така ознака не повинна обов'язково мати найбільшу амплітуду: слабка, але корельована з даними складова сигналу може бути значно інформативнішою за потужну, але незалежну заваду.

Наукова новизна роботи полягає у запропонованому способі трактування ПЕМВН як багаторівневого відображення інформаційного вмісту через фізичні процеси технічного засобу з окремим виділенням інформаційного сліду та критерію його релевантності. На відміну від підходу, за якого побічний сигнал розглядається переважно як небезпечна енергетична величина, предметом аналізу є послідовність причинно пов'язаних перевірок: «інформаційна подія – фізична активність – ПЕМВ – канал поширення – вимірювана ознака – перевірка причинної залежності».

Узагальнену послідовність відбору інформаційно релевантних ознак ПЕМВ представлено на рис. 1. Спочатку фіксують інформаційну подію, наприклад зміну пікселя, натискання клавіші або передавання блока даних. Потім встановлюють фізичний процес, який цією подією керує – комутацію логічного стану, зміну струму, формування пакетної послідовності або матричне сканування. Після цього відшуковують ПЕМВ, що повторюється синхронно з подією, локалізується в певній смузі частот або має стійкий часовий шаблон. Лише після підтвердження причинного зв'язку ознака може вважатися інформаційно релевантною.



Рис. 1. Узагальнена послідовність відбору інформаційно релевантних ознак ПЕМВ.

Для практичної оцінки доцільно використовувати п'ять взаємопов'язаних критеріїв: причинну залежність від інформації; відтворюваність за повторних однакових подій; розрізняльність різних значень інформації; можливість виділення ознаки після поширення до точки вимірювання; стійкість до завад і нестабільності середовища. Така сукупність критеріїв є продуктивнішою за просте ранжування сигналів за амплітудою, оскільки безпосередньо відповідає кінцевому завданню: встановити можливість відтворення з перехопленого технічними засобами ПЕМВ конфіденційної інформації або обмежити невідомі дані.

Інформаційно релевантні ознаки ПЕМВ монітора

Відеотракт є особливо придатним для дослідження інформаційно релевантних ПЕМВ, оскільки передавання зображення має детерміновану часову організацію. У VGA, DVI та HDMI інформація про зображення реалізується сукупністю повторюваних електричних процесів, пов'язаних із відображенням пікселів, формуванням рядків і кадрів та роботою відповідних інтерфейсів. Практичні експерименти засвідчують, що інформаційно залежні складові можуть реєструватися безпосередньо поблизу кабелю або панелі ближньопольовим зондом і на відстані антеною з приймальним трактом [9, 10].

Першою групою ознак є спектральні компоненти, пов'язані з періодичними параметрами відеосигналу та здатні містити інформацію про його стан. Для дослідженої конфігурації DVI у роботі [10] виявлено виражену спектральну складову поблизу 324 МГц, що відповідає третій гармоніці піксельної частоти 108 МГц; застосування смугової фільтрації шириною 10 МГц із центральною частотою 324 МГц дало змогу відновити передане зображення. Отже, інформативність частоти визначається не самим фактом її наявності, а її залежністю від режиму формування відео. Це означає, що під час перевірки конкретного монітора необхідно шукати не «універсальну частоту ПЕМВ», а взаємозв'язок між частотним максимумом і параметрами відеорежиму [9, 10].

Другою групою є часові ознаки: період кадру, повторюваність рядків, сталі часові інтервали та кореляція між послідовними реалізаціями одного й того самого зображення. Для LCD-дисплеїв показано наявність інформаційно залежних смуг у діапазоні кількох сотень мегагерц; конкретне розташування залежить від пристрою, а для отримання придатного зображення використовувалися виявлення часових параметрів і усереднення декількох кадрів [10]. Таким чином, навіть за невисокого миттєвого



співвідношення сигнал/завада повторюваність відеоструктури сама стає джерелом додаткової інформативності.

Третьою групою є ознаки, пов'язані з кодованими даними TMDS. Для цифрових інтерфейсів DVI/HDMI інформація про колір не надходить у приймач як безпосередня аналогова яскравість; вона представлена послідовністю символів, параметри якої впливають на спектральні та часові характеристики ПЕМВ. У роботі [11] встановлено кількісний зв'язок між структурою TMDS та інформаційно залежною складовою, а в [12] показано, що багатосмугове узгодження та класифікація ознак можуть використовуватися для віднесення сигналів до різних TMDS-символів і, зрештою, для розрізнення кольорів пікселів.

Важливим результатом сучасних досліджень є зміщення акценту з пошуку одиничного «підозрілого» спектрального піка на пошук набору пов'язаних ознак. Наприклад, у [10] продемонстровано можливість реконструкції відео від двох однотипних блоків відображення за рахунок вузькосмугової багатодіапазонної обробки, а у [12] використовуються кілька суміжних смуг приймання, їх частотне узгодження та когерентне накопичення для вилучення кольорових ознак кожного пікселя. Це показує, що локальна слабкість однієї складової може компенсуватися структурною узгодженістю кількох складових.

Окремий напрям досліджень становлять методи встановлення наявності інформаційної складової у ПЕМВ без необхідності повного відновлення переданого зображення. Tosaka, Yamataka та Fukunaga запропонували визначати наявність інформації за результатами спектрального аналізу випромінюваного збурення [9]. Інший підхід передбачає визначення інформаційно придатної смуги частот шляхом комплексного аналізу спектра, кореляційних характеристик та співвідношення сигнал/завада [13], тоді як метод, запропонований у [14], ґрунтується на автоматизованому пошуку перспективної смуги за положенням спектрального центра. Застосування таких методів є важливим для захисного обстеження, оскільки дає змогу на попередньому етапі виявити інформаційно значущі ділянки спектра та визначити доцільність подальшого детального аналізу або відновлення інформації.

Отже, для монітора найбільш інформативними слід вважати не всі наявні випромінювання, а ті компоненти, які мають одночасно три властивості: прив'язаність до часової структури кадру, залежність від конкретного вмісту зображення та відтворюваність за повторних спостережень. Практично це означає, що під час профілювання монітора слід змінювати тестове зображення, відстежувати зміни спектральних компонентів, перевіряти їх синхронність із кадрами та визначати, чи зберігаються ці ознаки після просторового поширення до контрольної точки.

Інформаційно релевантні ознаки ПЕМВ клавіатури

Клавіатура становить окремий клас джерел ПЕМВ, оскільки конфіденційна інформація надходить до неї дискретними подіями, а внутрішня електроніка перетворює кожне натискання на сукупність часових переходів, матричного сканування та передавання коду клавіші. Для USB-клавіатур експериментальні роботи 2016–2018 рр. показали можливість вимірювання ПЕМВ від кабелю, оброблення захопленого сигналу та відновлення інформації про натиснуті клавіші [15].

Важливим раннім експериментальним підтвердженням можливості такого витоку є праця М. Vuagnoux та S. Pasini [7], у якій досліджено чотири різні механізми інформаційного прояву клавіатурних сигналів – переходи ліній, гармонічні складові та випромінювання, пов'язані з матричним скануванням. Саме для сучасного аналізу клавіатури цінним є не відтворення описаної авторами конкретної атаки, а виділення загального принципу: інформативною є та частина ПЕМВ, у якій фізичний процес оброблення натискання зберігає часову або структурну залежність від коду клавіші [7, 15].

Найбільш наочно цей принцип проявляється в матричному скануванні. Клавіші організовані у вигляді матриці рядків і стовпців; контролер послідовно активує стовпці та визначає стан рядків. Через довгі провідники матриці комутаційні імпульси можуть створювати вимірювані електромагнітні складові. Коли натиснута клавіша, поява події змінює часову структуру наступного циклу сканування; отже, зафіксована ПЕМВ може переносити інформацію принаймні про групу клавіш, що відповідають певному стовпцю [7]. Цей механізм важливий і для USB-клавіатур, оскільки матричне сканування виконується всередині самої клавіатури незалежно від зовнішнього протоколу обміну.

Фрагмент матричної структури клавіатури, на якій простежуються провідники рядків і стовпців представлено на рис. 2.

Змістовно важливо відокремити фізичну структуру від власне інформаційної ознаки. Провідник матриці сам по собі не є конфіденційним носієм. Інформативною стає зміна його сигналу тоді, коли вона стабільно виникає у відповідь на певну клавішну подію. Саме тому під час обстеження необхідно

порівнювати часові записи для різних клавіш, встановлювати повторювані пікові структури та визначати, яка частина шаблону змінюється разом із натисненням.

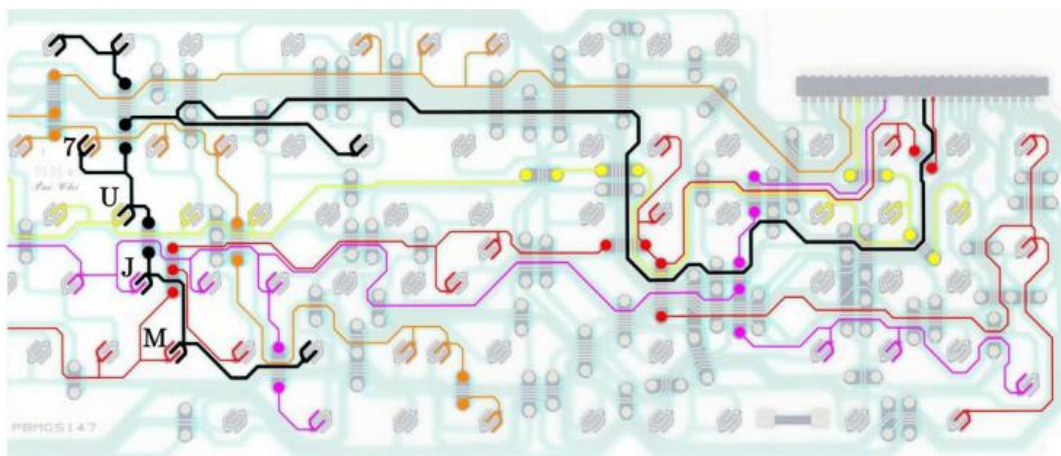


Рис. 2. Фрагмент матричної структури клавіатури, на якій простежуються провідники рядків і стовпців [7].

Для USB-клавіатур окрему групу ознак утворюють ПЕМВ сигнального кабелю, пов'язані з передаванням пакетів USB. В публікації [15] показано вимірювання випромінювань від кабелю USB-клавіатури та можливість відновлення інформації про натискання клавіш (рис. 3), розглянуто явище витоку, зумовлене механізмом передавання сигналу, та методи його оброблення. Додатково продемонстровано можливість автоматичного виявлення ПЕМВ із використанням автокореляції. Отже, для USB-клавіатури поряд із матричним скануванням інформативними можуть бути часові інтервали пакетних структур, повторюваність переходів та кореляція між реалізаціями сигналу.

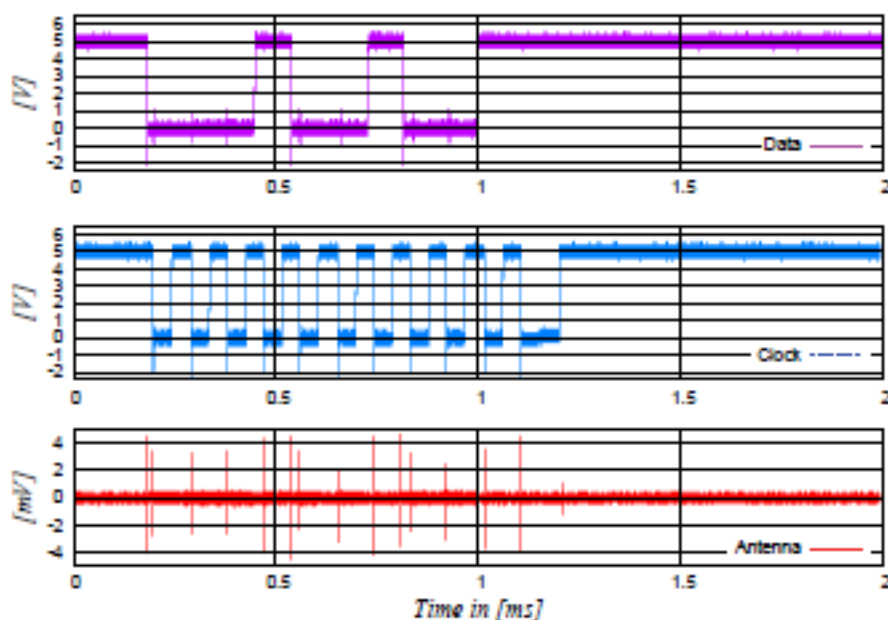


Рис. 3. Сигнали даних, тактовий сигнал і побічне електромагнітне випромінювання, зареєстровані в напівбезеховій камері для клавіатури A1 рамковою антеною (мідний провід завдовжки 1 м) на відстані 5 м під час натискання клавіші E (0x24). Сигнал даних: 00010010011 [7].

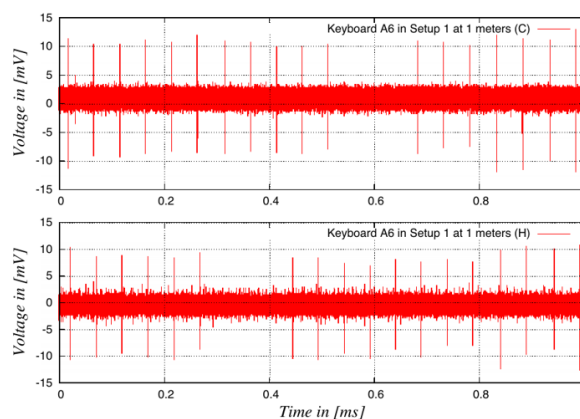


Рис. 4. Виміряні ПЕМВ матричного сканування для клавіш С і Н: відмінність часової структури пікових компонентів [7].

Відмінність часової структури пікових компонентів для клавіш С і Н (рис. 4) полягає не у загальному рівні фону, а у положенні та часовій послідовності виразних піків. Саме така ознака придатна для класифікації. При цьому не кожен пік необхідно трактувати як окремий символ; частина піків є стабільною структурою сканування, тоді як інформаційний компонент проявляється у зсуві або відсутності окремого імпульсу. Отже, інформативність визначається не окремою амплітудою, а структурою змін відносно опорного шаблону.

Ще один клас ознак – гармонічні та модульовані складові, пов’язані з внутрішніми тактовими процесами клавіатури. Гармоніки тактових процесів можуть бути модульовані залежно від стану даних. Для захисного обстеження це означає, що необхідно перевіряти не лише основні частоти цифрових переходів, а й їхні гармонічні складові та взаємозалежність амплітуди, частоти й часової позиції.

Отже, інформаційно релевантні ПЕМВ клавіатури доцільно локалізувати на двох рівнях. Перший – внутрішній: матричне сканування, переходи логічних станів, робота тактового генератора. Другий – зовнішній: передавання USB-пакетів кабелем і взаємодія кабелю з просторовим полем. Такий поділ дозволяє не помилково ототожнювати «сильне випромінювання» з найбільшою інформаційною цінністю: слабка, але синхронна з натисканням клавіші складова може бути значущішою за сильний, проте незалежний від події компонент.

Інформаційно релевантні ознаки ПЕМВ USB-інтерфейсу

USB-інтерфейс відрізняється від клавіатури тим, що інформація формується не лише внаслідок внутрішньої логіки пристрою, а й безпосередньо у процесі високошвидкісного цифрового обміну між контролерами. Для технічного захисту інформації принциповим є те, що корисна складова може бути присутня як у випромінюванні від кабелю, так і в сигналах, що поширюються проводовими шляхами. Сучасні огляди та експериментальні роботи розглядають USB як один із характерних фізичних каналів, у якому структура передавання може відображатися у побічному електромагнітному сигналі [16, 17].

Для USB-клавіатури інформаційним об’єктом є подія натискання та сформований нею код; для USB-накопичувача – послідовність байтів або блоків даних, що передаються під час обміну. Найінформативнішою ознакою в останньому випадку є залежна від даних структура цифрових переходів. У дослідженні [16] на експериментальному рівні показано можливість відновлення передаваних даних на бітовому рівні лише за ПЕМВ USB-обміну. Це принципово змінює підхід до оцінювання: для накопичувача потрібно перевіряти не тільки наявність сигналу поблизу кабелю, а й те, чи відрізняються вимірювані реалізації за різних блоків передаваних даних.

Окрему увагу слід приділяти проводовому шляху. У [17] розглянуто формування технічного каналу за рахунок проводового поширення побічних складових, а [14] узагальнює їх у TEMPEST-профілюванні. Такий шлях може бути стійкішим за просторовий у певних умовах, оскільки інформаційно залежна складова потрапляє до інших елементів системи через спільні електричні кола. Отже, під час захисного обстеження USB необхідно перевіряти щонайменше два класи точок: біля кабелю та роз’єму – для просторового поля, а також на доступних проводових ділянках – для оцінювання проводового каналу.

Для USB найбільш показовою є повторюваний зв’язок між структурою обміну та вимірюваним сигналом. Якщо один і той самий блок даних передається багаторазово, інформаційно значущі компоненти повинні повторюватися; якщо змінюється вміст блока, повинна узгоджено змінюватися

вимірювана ознака. Саме така контрольована варіація є ключовим доказом причинної залежності. Підхід узгоджується з TEMPEST-профілюванням, де профіль пристрою формується через співвіднесення його електромагнітного «відбитка» з функціональною активністю [17].

Узагальнення для USB можна сформулювати так: інформаційно релевантною є та частина ПЕМВ, яка зберігає ознаки дискретної структури обміну після проходження фізичного каналу. Для клавіатури це може бути часовий шаблон натискання та відповідного пакета; для накопичувача – послідовність переходів, що змінюється разом із передаваними бітами. Відповідно, вимірювальні прилади мають підбиратися не за максимальною чутливістю, а за здатністю зберігати потрібну часову та спектральну структуру.

В публікації [18], представлено результати експериментального визначення спектрального складу і енергетичних рівнів небезпечних сигналів, що виникають під впливом сигналів височастотного нав'язування (ВЧН). Аналіз спектрів інтермодуляційного випромінювання інтерфейсів монітора, принтера та USB (рис. 5), показують, що інформативні компоненти небезпечних сигналів підсилюються за рахунок впливу сигналів височастотного нав'язування, полегшуючи перехоплення конфіденційної інформації.



Рис. 5. Спектри інтермодуляційного випромінювання інтерфейсів монітора, принтера та USB під впливом сигналу ВЧН [18].

5. Узагальнення ознак та правило встановлення інформаційної релевантності

Таблиця 1

Ознаки інформаційної релевантності джерел

Джерело	Інформаційна подія	Найінформативніші ознаки	Типовий канал поширення
Відеотракт	Формування пікселів, рядків і кадрів	піксельна/кадрова розгортка; TMDS–символи; часові інтервали; повторюваність кадрів	просторове поле біля кабелю/панелі; частково провідні шляхи
Клавіатура	Натискання клавіші; матричне сканування; передавання коду	пікові часові шаблони; зсуви імпульсів; гармоніки; пакетні структури; автокореляція	поле біля кабелю та корпусу; провідний шлях
USB–накопичувач	Передавання блоків даних	переходи, зумовлені зміною даних; бітові послідовності; повторюваність обміну; часові шаблони	кабель, роз'єм, просторове поле та провідний канал



Із представлених результатів випливає загальне правило: ПЕМВ стає об'єктом технічного захисту інформації не в момент перевищення певного рівня напруженості поля, а в момент встановлення стійкої відповідності між фізичною ознакою сигналу та невідомим значенням інформації. Така відповідність має бути експериментально перевірена зміною тестових даних. Якщо зміна інформації спричиняє узгоджену зміну ознаки, а сама ознака відтворюється при повторних вимірюваннях і залишається розрізняваною на тлі завад, ПЕМВ слід вважати інформаційно релевантним.

Практично це означає, що процедура профілювання ПК повинна будуватися від інформації до сигналу, а не навпаки. Для відеотракту спочатку змінюють тестове зображення, для клавіатури – послідовність контрольованих натискань, для USB-накопичувача – вміст тестового блока. Далі визначають, які часові, спектральні чи кореляційні характеристики реагують на ці зміни. На наступному етапі перевіряють, який фізичний канал зберігає ознаку – просторовий чи провідний. Лише після цього доцільно оцінювати можливість відновлення даних або ступінь обмеження простору можливих значень. Така послідовність мінімізує ризик хибного трактування сильних, але неінформативних складових як небезпечних для конфіденційності.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Аналіз публікацій показує, що для персонального комп'ютера інформаційно релевантні ПЕМВ формуються не як однорідна сукупність «випромінювань від пристрою», а як набір фізичних проявів конкретних інформаційних подій. У відеотракті ключовими ознаками є спектральні складові, зумовлені тактовою частотою піксельного потоку та параметрами кадрової розгортки; для цифрових інтерфейсів із передаванням даних за допомогою TMDS додатковими ознаками є структура символів і закономірності їх повторення під час передавання послідовних кадрів. Для клавіатури основну інформаційну цінність мають часові шаблони матричного сканування, переходи, пов'язані з кодуванням клавіші, гармонічні складові та параметри USB-обміну. Для USB-накопичувачів найбільш істотним є збереження в ПЕМВ залежності від передаваних бітів і пакетної структури обміну, причому така залежність може проявлятися як у просторовому полі, так і в провідному каналі.

Отже, для завдань технічного захисту інформації доцільно переходити від оцінювання загального рівня ПЕМВ до цілеспрямованого пошуку інформаційно релевантних ознак. Запропонована послідовність «інформаційна подія – фізична активність – ПЕМВ – канал поширення – вимірювана ознака – перевірка причинної залежності» дає змогу встановлювати, в яких параметрах ПЕМВ може потенційно міститися конфіденційна інформація та за якими вимірювальними ознаками їх доцільно перевіряти. Саме така причинно-структурна інтерпретація створює основу для обґрунтованого вибору точок контролю, смуг вимірювання та методів оброблення сигналів.

Перспективним напрямом є дослідження інформаційно релевантних ознак акустоелектричних каналів витоку інформації, що утворюються шляхом паразитного перетворення акустичних сигналів в електричні на електронних компонентах технічних засобів та систем, розташованих на об'єктах інформаційної діяльності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. TR TZI – PEMVN-95: *Temporary recommendations on technical protection of information against leakage through channels of unintentional electromagnetic emanations and coupling*. (1995).
2. Zabolotnyi, V. I., Oleinikov, A. M., Zabolotnyi, D. M., & Kustov, A. K. (2024). Tekhnichnyi kanal vytku informatsii pobichnymy elektromagnitnymy perevyprominiuvanniamy dopomizhnykh tekhnichnykh zasobiv i system. *Radiotekhnika*, 218, 56–63. <https://doi.org/10.30837/rt.2024.3.218.04>
3. *Counterintelligence glossary: Terms & definitions of interest for CI professionals*. (n.d.). <https://irp.fas.org/eprint/ci-glossary.pdf>
4. van Eck, W. (1985). Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security*, 4(4), 269–286. <http://cryptome.org/emr.pdf>
5. Kuhn, M. G. (2005). Electromagnetic eavesdropping risks of flat-panel displays. In *Privacy enhancing technologies: 4th International Workshop, PET 2004, Toronto, Canada, May 26–28, 2004, revised selected papers* (pp. 88–107). Springer.
6. Kuhn, M. G., & Anderson, R. J. (1998). Soft TEMPEST: Hidden data transmission using electromagnetic emanations. In D. Aucsmith (Ed.), *Information hiding* (Lecture Notes in Computer Science, Vol. 1525, pp. 124–142). Springer-Verlag. <http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf>
7. Vuagnoux, M., & Pasini, S. (2009). Compromising electromagnetic emanations of wired and wireless keyboards. In *18th USENIX Security Symposium (USENIX Security 09)* (pp. 1–16). https://www.usenix.org/event/sec09/tech/full_papers/sec09_attacks.pdf



8. Kubiak, I., Przybysz, A., & Musial, S. (2020). Possibilities of electromagnetic penetration of displays of multifunction devices. *Computers*, 9(3), Article 62. <https://doi.org/10.3390/computers9030062>
9. Tosaka, T., Yamanaka, Y., & Fukunaga, K. (2011). Method for determining whether or not information is contained in electromagnetic disturbance radiated from a PC display. *IEEE Transactions on Electromagnetic Compatibility*, 53(2), 318–324. <https://doi.org/10.1109/TEM.2010.2103562>
10. Lee, H. S., Yook, J.-G., & Sim, K. (2016). Study for possibility of information leakage from digital video display interface. In *2016 URSI Asia-Pacific Radio Science Conference (URSI AP-RASC)* (pp. 1102–1103). <https://doi.org/10.1109/URSIAP-RASC.2016.7601327>
11. Lee, E., Choi, D.-H., Nam, T., & Yook, J.-G. (2022). A quantitative analysis of compromising emanation from TMDS interface and possibility of sensitive information leakage. *IEEE Access*, 10, 73997–74011. <https://doi.org/10.1109/ACCESS.2022.3184294>
12. Erdeljan, D., & Kuhn, M. G. (2025). Multiband pixel colour classification from HDMI emissions. In *2025 International Symposium on Electromagnetic Compatibility – EMC Europe* (pp. 778–783). <https://www.repository.cam.ac.uk/items/a4115966-0613-498e-8915-3d4b229bf985>
13. Du, Y.-L., Lü, Y.-H., Zhang, J.-L., & Zhang, N. (2013). Method for determining the best frequency band for eavesdropping the display image of a PC. *Journal of China Universities of Posts and Telecommunications*, 20(4), 93–98. [https://doi.org/10.1016/S1005-8885\(13\)60075-8](https://doi.org/10.1016/S1005-8885(13)60075-8)
14. Sun, D., Shi, J., Wei, D., & Zhang, M. (2014). A low-cost and efficient method of determining the best frequency band for video leaking signal reconstruction. In *2014 2nd International Conference on Systems and Informatics (ICSAI)* (pp. 624–628). <https://doi.org/10.1109/ICSAI.2014.7009361>
15. Boitan, A., Bărtușică, R., Halunga, S., Popescu, M., & Ionuță, I. (2018). Compromising electromagnetic emanations of wired USB keyboards. In O. Fratu et al. (Eds.), *Future access enablers for ubiquitous and intelligent infrastructures: FABULOUS 2017* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol. 241, pp. 39–44). Springer. https://eudl.eu/pdf/10.1007/978-3-319-92213-3_6
16. Boitan, A., Halunga, S., Bîndar, V., & Fratu, O. (2022). Compromising electromagnetic emanations of USB mass storage devices. *Wireless Personal Communications*, 126, 97–122. <https://doi.org/10.1007/s11277-020-07329-8>
17. Antić, V., Protić, D., Stanković, M., Prodanović, R., Manić, M., Ostojić, G., Stankovski, S., & Kučević, D. (2024). Protecting data at risk of unintentional electromagnetic emanation: TEMPEST profiling. *Applied Sciences*, 14(11), Article 4830. <https://doi.org/10.3390/app14114830>
18. Kriuchkova, L., Tsmokanych, I., Mazur, N., & Chernihivskiy, I. (2025). Spectral characteristics of intermodulation emissions during high-frequency imposition. *Cybersecurity Providing in Information and Telecommunication Systems*, 3991, 449–462. <https://elibrary.kubg.edu.ua/id/eprint/52537/>

**Monakhov Dmytro**

graduate student

Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine

ORCID: 0009-0002-3471-4194

monakdim@ukr.net

Kriuchkova Larysa

Doctor of technical sciences, professor

Professor of the Volodymyr Buriachok Department of Information and Cyber Security

Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine

ORCID: 0000-0002-8509-6659

l.kriuchkova@kubg.edu.ua

INFORMATION-RELEVANT FEATURES OF UNINTENTIONAL ELECTROMAGNETIC EMANATIONS FROM A PERSONAL COMPUTER

Abstract. The operation of any information-processing equipment gives rise to a number of unintended technical channels through which information may leak. Among the most common and potentially hazardous are channels associated with unintentional electromagnetic emanations and conducted coupling. The conventional approach to protecting information against leakage through such channels is primarily focused on detecting potentially compromising emanations and determining the conditions under which they can be exploited to obtain information. At the same time, an important task is to identify, among the various unintended signals, those features that exhibit a stable relationship with confidential data and can be intercepted by technical intelligence means. The aim of this study is to investigate information-relevant features of unintentional electromagnetic emanations generated by personal computer components in order to support information protection at information-processing facilities. The study considers unintentional electromagnetic emanations from a personal computer as a technical information leakage channel. Emanations associated with the display video path, keyboard, and USB interface are analysed. It is shown that the information relevance of an emanation is determined not by its absolute level, but by its causal dependence on the information content, its temporal and spectral structure, reproducibility, ability to propagate through radiated or conducted paths, and robustness against interference. For video signals, the principal features are associated with the pixel clock, frame scanning parameters, and TMDS symbols; for keyboards, they include signal transitions, keyboard-matrix scanning, and features associated with key-code transmission; and for USB interfaces, they include data-dependent differential transitions and the packet structure of data exchange. A generalized procedure for identifying information-relevant features is proposed. The procedure makes it possible to determine which parameters of unintentional electromagnetic emanations may potentially convey confidential information and which measurable features should be examined when assessing such emanations.

Keywords: information technology; confidential information; unintentional electromagnetic emanations; technical information leakage channel; technical information protection; video signal; information-relevant feature; electromagnetic compatibility.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. TR TZI – PEMVN-95: *Temporary recommendations on technical protection of information against leakage through channels of unintentional electromagnetic emanations and coupling*. (1995).
2. Zabolotnyi, V. I., Oleinikov, A. M., Zabolotnyi, D. M., & Kustov, A. K. (2024). Tekhnichniy kanal vytku informatsii pobichnymi elektromagnitnymi perevyprominiuvanniamy dopomizhnykh tekhnichnykh zasobiv i system. *Radiotekhnika*, 218, 56–63. <https://doi.org/10.30837/rt.2024.3.218.04>
3. *Counterintelligence glossary—Terms & definitions of interest for CI professionals*. (n.d.). <https://irp.fas.org/eprint/ci-glossary.pdf>



4. van Eck, W. (1985). Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security*, 4(4), 269–286. <http://cryptome.org/emr.pdf>
5. Kuhn, M. G. (2005). Electromagnetic eavesdropping risks of flat-panel displays. In *Privacy enhancing technologies: 4th International Workshop, PET 2004, Toronto, Canada, May 26–28, 2004, revised selected papers* (pp. 88–107). Springer.
6. Kuhn, M. G., & Anderson, R. J. (1998). Soft TEMPEST: Hidden data transmission using electromagnetic emanations. In D. Aucsmith (Ed.), *Information hiding* (Lecture Notes in Computer Science, Vol. 1525, pp. 124–142). Springer-Verlag. <http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf>
7. Vuagnoux, M., & Pasini, S. (2009). Compromising electromagnetic emanations of wired and wireless keyboards. In *18th USENIX Security Symposium (USENIX Security 09)* (pp. 1–16). https://www.usenix.org/event/sec09/tech/full_papers/sec09_attacks.pdf
8. Kubiak, I., Przybysz, A., & Musial, S. (2020). Possibilities of electromagnetic penetration of displays of multifunction devices. *Computers*, 9(3), 62. <https://doi.org/10.3390/computers9030062>
9. Tosaka, T., Yamanaka, Y., & Fukunaga, K. (2011). Method for determining whether or not information is contained in electromagnetic disturbance radiated from a PC display. *IEEE Transactions on Electromagnetic Compatibility*, 53(2), 318–324. <https://doi.org/10.1109/TEMC.2010.2103562>
10. Lee, H. S., Yook, J.-G., & Sim, K. (2016). Study for possibility of information leakage from digital video display interface. In *2016 URSI Asia-Pacific Radio Science Conference (URSI AP-RASC)* (pp. 1102–1103). <https://doi.org/10.1109/URSIAP-RASC.2016.7601327>
11. Lee, E., Choi, D.-H., Nam, T., & Yook, J.-G. (2022). A quantitative analysis of compromising emanation from TMDS interface and possibility of sensitive information leakage. *IEEE Access*, 10, 73997–74011. <https://doi.org/10.1109/ACCESS.2022.3184294>
12. Erdeljan, D., & Kuhn, M. G. (2025). Multiband pixel colour classification from HDMI emissions. In *2025 International Symposium on Electromagnetic Compatibility – EMC Europe* (pp. 778–783). <https://www.repository.cam.ac.uk/items/a4115966-0613-498e-8915-3d4b229bf985>
13. Du, Y.-L., Lü, Y.-H., Zhang, J.-L., & Zhang, N. (2013). Method for determining the best frequency band for eavesdropping the display image of a PC. *Journal of China Universities of Posts and Telecommunications*, 20(4), 93–98. [https://doi.org/10.1016/S1005-8885\(13\)60075-8](https://doi.org/10.1016/S1005-8885(13)60075-8)
14. Sun, D., Shi, J., Wei, D., & Zhang, M. (2014). A low-cost and efficient method of determining the best frequency band for video leaking signal reconstruction. In *2014 2nd International Conference on Systems and Informatics (ICSAI)* (pp. 624–628). <https://doi.org/10.1109/ICSAI.2014.7009361>
15. Boitan, A., Bărtușică, R., Halunga, S., Popescu, M., & Ionuță, I. (2018). Compromising electromagnetic emanations of wired USB keyboards. In O. Fratu et al. (Eds.), *Future access enablers for ubiquitous and intelligent infrastructures: FABULOUS 2017* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol. 241, pp. 39–44). Springer. https://eudl.eu/pdf/10.1007/978-3-319-92213-3_6
16. Boitan, A., Halunga, S., Bîndar, V., & Fratu, O. (2022). Compromising electromagnetic emanations of USB mass storage devices. *Wireless Personal Communications*, 126, 97–122. <https://doi.org/10.1007/s11277-020-07329-8>
17. Antić, V., Protić, D., Stanković, M., Prodanović, R., Manić, M., Ostojić, G., Stankovski, S., & Kučević, D. (2024). Protecting data at risk of unintentional electromagnetic emanation: TEMPEST profiling. *Applied Sciences*, 14(11), 4830. <https://doi.org/10.3390/app14114830>
18. Kriuchkova, L., Tsmokanych, I., Mazur, N., & Chernihivskyi, I. (2025). Spectral characteristics of intermodulation emissions during high-frequency imposition. *Cybersecurity Providing in Information and Telecommunication Systems*, 3991, 449–462. <https://elibrary.kubg.edu.ua/id/eprint/52537/>

Отримано редакцією журналу / Received: 12.03.26

Прорецензовано / Revised: 27.03.26

Схвалено до друку / Accepted: 24.09.26



This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.