

Конотопець Микола Миколайович (кандидат технічних наук, доцент)¹

Самойлов Ігор Володимирович (кандидат технічних наук, доцент)¹

Сторчак Антон Сергійович (кандидат технічних наук)¹

Смольков Олександр Юрійович (кандидат технічних наук)²

¹ Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна

² Національний університет оборони України, Київ, Україна

ПРОПОЗИЦІЇ З УДОСКОНАЛЕННЯ ТЕХНІЧНИХ ХАРАКТЕРИСТИК АНАЛІЗАТОРІВ СПЕКТРУ СИГНАЛІВ

Метою статті є розроблення пропозицій з удосконалення технічних характеристик аналізаторів спектра сигналів для виявлення, оцінювання та аналізу електромагнітних полів, які виникають у процесі роботи технічних засобів обробки інформації на об'єктах інформаційної діяльності та можуть служити джерелом інформації для зловмисників. Під час написання статті застосовано методи аналізу і порівняння для розгляду побудови та порівняння технічних характеристик існуючих аналізаторів спектра сигналів. Наведений математичний апарат дав змогу проаналізувати математичні залежності параметрів виявлення небезпечних сигналів аналізаторами спектра сигналів на основі характеристик приймача. За допомогою методу синтезу розроблено пропозиції стосовно удосконалення технічних характеристик аналізаторів спектра сигналів. Також із використанням технічних і технологічних методів виявлення та оцінки побічних електромагнітних випромінювань й наведень, які можуть виникати в процесі роботи радіоелектронних засобів обробки, зберігання та обміну інформації на об'єктах інформаційної діяльності, формалізовано модель виявлення побічних електромагнітних випромінювань і наведень небезпечних сигналів за енергетичним критерієм, що містить основні фізичні характеристики приймача. У статті розроблено пропозиції з удосконалення технічних характеристик аналізатора спектра сигналів для виявлення та оцінки побічних електромагнітних випромінювань і наведень. Перебуваючи у складі апаратних або апаратно-програмних комплексів, призначених для вирішення завдань інструментального контролю, аналізатори спектра сигналів здійснюють виявлення, оцінювання (вимірювання) та аналіз просторово-частотних характеристик небезпечних сигналів, що виникають у процесі роботи радіоелектронних засобів обробки інформації на об'єктах інформаційної діяльності. Такі сигнали, в свою чергу, можуть характеризувати джерела побічних електромагнітних випромінювань і наведень, та розглядати їх як складову потенційних можливих технічних каналів витоку інформації. Розроблено формалізовану модель виявлення побічних електромагнітних випромінювань і наведень на об'єктах інформаційної діяльності за енергетичним критерієм на основі теорії виявлення та розпізнавання сигналів з урахуванням зовнішніх і внутрішніх шумів. Науковою новизною є конкретизація відомих даних та їх поширення на нові об'єкти дослідження, якими є власні побічні електромагнітні випромінювання і наведення від струмів інформативних сигналів засобів обробки інформації, що можуть бути використані на об'єктах інформаційної діяльності. Практичною і теоретичною значущістю отриманих результатів дослідження у військовій та технічній сферах є отримання знань щодо можливостей підвищення якісних характеристик контрольно-виміральної техніки і визначеної послідовності дій для унеможливлення перехоплення інформації зловмисниками. Ці результати можуть бути використані на об'єктах інформаційної діяльності в сучасних умовах.

Ключові слова: радіоелектронні засоби, засоби обробки інформації, аналізатор спектра сигналів, амплітудно-частотна характеристика, небезпечний сигнал, технічні канали витоку інформації, радіохвильовий контроль, апаратні засоби, апаратно-програмний комплекс, діаграма спрямованості антени.

Вступ

Розвиток обчислювальної техніки і широке її використання практично у всіх сферах діяльності підприємств різних форм власності по новому поставили питання про методи і засоби шпигунства з місць обробки і зберігання інформації. Через це

усі об'єкти інформаційної діяльності стали посідати чільне місце як об'єкти інформаційної розвідки, а в радіоелектронній розвідці з'явився окремий її вид – розвідка побічних електромагнітних випромінювань та наведень (далі – ПЕМВН).

Розвідка ПЕМВН це різновид пасивної радіоелектронної розвідки (далі – РЕР), яка забезпечує отримання відомостей про противника шляхом виявлення та аналізу сигналів за рахунок використання радіоелектронної апаратури, що реєструє побічні електромагнітні випромінювання, наведення та електричні сигнали, які можуть наводитись первинними електромагнітними випромінюваннями в струмопровідних колах різних технічних пристроїв та конструкціях будівель. Зазначені ефекти утворюють технічні канали витоку інформації, що вимагають їх дослідження і доведення до безпечного стану, що визначений вимогами та нормами захищеності. Одним із завдань щодо убезпечення інформації від витоку технічними каналами є їх своєчасне виявлення з подальшим визначенням конкретних заходів щодо їх нейтралізації.

Постановка проблеми. На сьогодні у виробників радіоелектронної техніки зберігається стійка потреба у пристроях з дедалі більшою продуктивністю, малим енергоспоживанням та компактними розмірами. Реалізувати її дозволяють радіочастотні та мікрохвильові друковані плати – це тип друкованих плат, які у своїй роботі під час передавання, приймання, оброблення та зберігання інформації використовують радіочастотний або мікрохвильовий сигнал, що відповідає лінійці частот від мегагерц до гігагерц. Як відомо, ці діапазони можуть бути задіяні в роботі засобів мобільного зв'язку, радіонавігації, військових та цивільних радарів і низки інших засобів, на яких може здійснюватися обробка конфіденційної інформації. Тому цей клас пристроїв можна вважати джерелами ПЕМВН, і розглядати як складову *потенційних можливих технічних каналів витоку інформації*.

В умовах жорсткої промислової конкуренції та зростання попиту на друковані плати, конструкція і технологія складання електронних модулів на їх базі – «електронне складання» (electronic assembly) безперервно вдосконалюється. Основними напрямками розвитку сучасних і конструктивних рішень друкованих плат на сьогодні стало [1]:

освоєння проектувальниками та виробниками більш високих тактових частот, що зумовлює, з одного боку, більшу пропускну спроможність, а з іншого – частоти, на яких можуть існувати *інформативні сигнали ПЕМВН*;

збільшення ступеню інтеграції електронних виробів (вища інтеграція функцій на кремнії), що призвело до можливості збільшення виводів вхід/вихід (1/10) – понад 1000 виводів на корпус електронних виробів та поверхнево-вмонтованих компонентів (далі – ПМК), що дозволяє розглядати їх як випадкові антени *інформативних сигналів ПЕМВН*;

зменшення кроку розташування виводів електронних виробів, що може призвести до появи паразитних наведень;

збільшення тепловиділення електронних

виробів у зв'язку з підвищенням їх функціональної складності та інші.

В свою чергу, знання основних напрямів розвитку схемотехнічних та конструктивних рішень друкованих плат, які використовуються в пристроях приймання обробки та зберігання інформації дасть змогу глибше розуміти фізичні принципи їх роботи, а також удосконалювати засоби та методи виявлення, оцінки та розпізнавання сформованих ними ПЕМВН, як *джерел технічних каналів витоку інформації*.

Тому дослідження об'єкта інформаційної діяльності (далі – ОІД) щодо виявлення потенційно можливих каналів витоку інформації за рахунок ПЕМВН залишається одним з найбільш актуальних завдань у сфері технічного захисту інформації. Істотно полегшити його вирішення дають змогу аналізатори спектру сигналів. Вони являють собою спеціалізовані високочутливі прилади з можливістю багатоканальної, в тому числі кореляційної, обробки спектральних складових та візуалізації результатів.

Аналіз останніх досліджень і публікацій. У роботі [2], голландського вченого-комп'ютерника Wim van Eck (Вим ван Ейк) вперше були наведені результати дослідження можливості «крадіжки» інформації з відеодисплеїв шляхом перехоплення та декодування ненавмисних електромагнітних випромінювань та наведень, що утворюються таким типом обладнання при їх функціонуванні. Цей метод перехоплення інформації привернув увагу спільноти комп'ютерної безпеки та широкої громадськості, що призвело до популяризації терміну Van Eck Phreaking («Ван-Ек Фрейкінг»).

Найбільш докладно дослідження проблеми перехоплення побічних електромагнітних випромінювань та наведень відеомоніторів з інтерфейсами VGA і DVI провів в своїй дисертації М. Г. Кун (Markus G. Kuhn) [3]. Для перехоплення небезпечних сигналів він використовував цифровий супергетеродинний приймач з амплітудним демодулятором Dynamic Sciences R1250 з логічно-періодичною антеною. Діапазон частот приймача становив від 100 Гц до 1 ГГц, а смуга пропускання від 50 Гц до 200 МГц. Наявність смуги пропускання 200 МГц дала змогу приймати і демодулювати імпульсні сигнали тривалістю до 5 нс. Як показник оцінювання можливості перехоплення побічних електромагнітних випромінювань та наведень було використано критерій Неймана-Пірсона (імовірність правильного виявлення інформативного сигналу приймальним пристроєм засобу зловмисника P_o за фіксованим значенням хибної тривоги P_{xt}).

Peter Smulders в своїй роботі [4] показав, що не тільки побічні електромагнітні випромінювань та наведень відеомоніторів з інтерфейсами VGA і DVI є вразливим до перехоплення на відстані, а що в деяких випадках можна перехоплювати сигнали даних, що проходять по кабелю RS-232, шляхом перехоплення та розшифровки електромагнітного випромінювання. На користь цього твердження

діють багато факторів: Амплітуда бітів сигналу даних RS-232 є відносно велика в порівнянні з рівнями логічних сигналів, що використовуються у внутрішніх схемах обладнання. Час наростання і спаду сигналу даних дуже короткі. Отже, вони відповідають високочастотним компонентам, що призводить до значне випромінювання. Незбалансоване відносно землі підключення інтерфейсу RS-232 сприятиме високому рівню випромінювання. Кабелі RS-232, у багатьох випадках, не екрановані, або екрановані ненадежним чином. Внутрішні стіни приміщень (без металевих решіток) суттєво не впливають на рівень випромінювання на частотах нижче 200 МГц.

Martin Vuagnoux та Sylvain Pasini в статті [5] проаналізували побічні електромагнітні випромінювання та наведення комп'ютерних клавіатур, які часто використовуються для передачі конфіденційних даних, таких як паролі. Їх підхід полягає в отриманні необробленого сигналу безпосередньо з антени та обробці всього захопленого електромагнітного спектру. Завдяки цьому методу було виявлено чотири різні типи компрометуючих електромагнітних випромінювань, створених дротовими та бездротовими клавіатурами. Ці викиди призводять до повного або часткового відновлення натискань клавіш. Отже, вони небезпечні для передачі конфіденційної інформації.

В своїх подальших дослідженнях [6] Markus G. Kuhn показав, що побічні електромагнітні випромінювання та наведень можуть бути перехоплені не лише з комп'ютерних дисплеїв, основою яких служать електронно-променеві трубки, а і з сучасних плоских дисплеїв. Вони так само керуються повторюваними відеосигналами в частотних діапазонах, де навіть екрановані кабелі випромінюють радіохвилі, які можна виявити в навколишній середовищі за допомогою спрямованих антен і широкосмугових приймачів. Послідовні формати передачі даних зі швидкістю 1 Гбіт/с, що використовуються цифровими відеоінтерфейсами, фактично модулюють сигнал, роблячи його ще більш придатним для віддаленого прийому, ніж випромінювання аналогових систем.

Публікація [7] висвітлює методологію оцінки побічних електромагнітних випромінювань та наведень мобільного пристрою, що тестується. Вказані авторами випромінювання потенційно можуть містити інформацію для відтворення зображень з екрана. Основна ідея роботи полягає в тому, щоб використовувати статистичний тест замість реконструкції зображень на екрані. Валідність представленої методології продемонстровано в реальних умовах експериментом зі спостереження за електромагнітним випромінюванням екрана планшета, яке може бути використано в атаці TEMPEST.

У науковій роботі [8] продемонстровано, що безпека конфіденційної інформації може бути

порушена через ненавмисні електромагнітні випромінювання від інформаційно-технологічного обладнання (ІТО), яке використовується для її обробки. Описано розробку системи нечіткого виведення, яка може бути використана для оцінки ймовірності випромінювання та кондуктивного впливу ненавмисних електромагнітних випромінювань на вразливість. Система має потенціал стати цінним інструментом для фахівців з кібербезпеки, які не мають досвіду роботи з радіочастотами. Система була протестована на офісних пристроях ІТЕ і виявилася ефективною в прогнозуванні ймовірності виникнення випромінюваних і кондуктивних вразливостей.

Ураховуючи вище зазначене дослідження стосовно підвищення якості виявлення та нейтралізації побічних електромагнітних випромінювань та наведень, що виникають у процесі роботи технічних засобів обробки інформації і можуть бути використані на об'єктах інформаційної діяльності в сучасних умовах є актуальним науковим завданням.

Метою статті є розроблення пропозицій з удосконалення технічних характеристик аналізаторів спектра сигналів для виявлення, оцінювання та аналізу електромагнітних полів, які виникають у процесі роботи технічних засобів обробки інформації на об'єктах інформаційної діяльності та можуть служити джерелом інформації для зловмисників.

Виклад основного матеріалу дослідження

На сьогоднішній день в арсеналі дослідників радіосигналів використовуються амплітудні аналізатори спектра, векторні аналізатори спектра та аналізатори спектра в реальному масштабі часу. Всі вони мають свої переваги та недоліки при дослідженні конкретних видів сигналів. Так, за принципом своєї побудови амплітудні аналізатори спектра поділяють на: аналізатори *спектру послідовного типу та аналізатори спектра паралельного типу*. Аналізатори спектра послідовного типу побудовані на базі супергетеродинів що автоматично перестроюються. Це такий тип радіоприймачів, які перетворюють сигнал що надходить, в сигнал фіксованої проміжної частоти та в подальшому посилюють її. Отже, шляхом застосування принципу супергетеродинного перетворення частоти сигналу, що аналізується, виявляється можливим здійснювати послідовний зсув частот його спектральних складових відносно вузькосмугової вибіркової системи, що має фіксовану частоту налаштування. Такі аналізатори є найбільш простими за своєю апаратною реалізацією і забезпечують широкий динамічний діапазон, однак мають той суттєвий недолік, що в кожен момент дані амплітуди розраховуються тільки в одній точці.

Звичайні супергетеродинні аналізатори спектра сигналу послідовного типу раніше у своїй конструкції використовували виключно аналогові

компоненти. У процесі свого вдосконалення вони отримали такі цифрові елементи як аналогово-цифрові перетворювачі (АЦП), засоби цифрового оброблення сигналів і мікропроцесори. Але основний принцип дії залишився без змін і найкраще підходив для дослідження стаціонарних сигналів.

Для отримання амплітудно-частотної характеристики, на виході супергетеродинного аналізатора спектра сигналів, у них виконується дворазове і більше перетворення частоти досліджуваного сигналу з подальшою його фільтрацією смуговим фільтром. Вибір смуги пропускання фільтра визначає роздільну здатність аналізатора спектра сигналу.

Далі використовуючи амплітудний детектор виділяється амплітуда сигналу на кожній частоті аналізованої ділянки спектра. Цей метод дає змогу охопити широкий динамічний діапазон частот, але має істотний недолік. У кожен момент часу дані амплітуди сигналу розраховуються тільки в одній точці. Для аналізу всього досліджуваного діапазону частот аналізатору необхідно перелаштовувати робочу частоту, що потребує певного часу. У деяких випадках це може складати до декількох секунд. Цей підхід ґрунтується на припущенні, що за час, поки аналізатор виконує кілька циклів розгортки, вимірюваний сигнал не зазнає істотних змін. Отже, потрібен відносно стабільний вхідний сигнал, що не змінюється. Якщо ж у сигналі є швидкі зміни, цілком ймовірно, що вони будуть пропущені.

В аналізаторах спектра з послідовною перебудовою частоти не забезпечується синхронізація за нестаціонарним сигналом і не зберігається повний запис залежності сигналу від часу. Забезпечити досить малі значення нелінійності та шуму аналого-цифрових перетворювачів (далі – АЦП) – завдання непросте, хоча водночас усуваються деякі види похибок, властивих суто аналоговим аналізаторам спектра.

Подальшим кроком удосконалення аналізаторів спектра сигналів стали векторні аналізатори. На відміну від аналізаторів спектра сигналу з послідовною перебудовою частоти, де виконуються скалярні виміри амплітуди вхідного сигналу, векторні аналізатори спектра сигналу забезпечують аналіз сигналів із цифровою модуляцією, вимірюючи амплітуду і фази досліджуваного сигналу. Однак, більшість векторних аналізаторів сигналів (хоча й не всі) призначені для збирання миттєвих знімків вхідного сигналу в довільні моменти часу, що ускладнює, а то й унеможлиблює, завдання збереження тривалого запису послідовних вибірок для кореляційного накопичення інформації про зміну сигналу з плином часу. Як і в аналізаторах спектра з розгорткою, можливості синхронізації обмежені синхронізацією на проміжній частоті та зовнішньою синхронізацією.

Ще одним параметром, за яким поділяють аналізатори спектра є частотний діапазон, за яким існують широкосмугові радіочастотні аналізатори, аналізатори оптичного діапазону та акустичні або низькочастотні аналізатори. Останні два класи в даній статті не беруться до уваги, бо в якості інформативних сигналів розглядаються радіочастотні сигнали.

Сучасні ж завдання вимірювання радіосигналів вимагають вивчення зміни частоти, амплітуди та параметрів модуляції на коротких і тривалих інтервалах часу для надійного опису динамічного радіочастотного сигналу, що виробляється пристроєм. Завдяки існуванню *аналізаторів спектру сигналу з обробкою в реальному масштабі часу під час вимірювань враховується ще один важливий параметр – час*. Це дає змогу вирішувати у процесі досліджень такі завдання:

захоплення й аналіз нестаціонарних і динамічних сигналів;

захоплення пакетної передачі, викидів, перехідних процесів під час перемикання;

визначення часу встановлення системи АП (дрейфу частоти, мікрофонного ефекту);

виявлення короткочасних перешкод, аналіз шуму;

захоплення сигналів з розподіленим спектром і сигналів зі стрибкоподібною перебудовою частоти.

моніторинг використання спектра, виявлення сторонніх передач;

випробування на сумісність, діагностика електромагнітних завад.

Наведений перелік дає змогу досліджувати небезпечні інформативні сигнали, які можуть виникати в технічному каналі витоку інформації за рахунок побічних електромагнітних випромінювань та наведень. Вдосконалення таких *аналізаторів спектру сигналу з обробкою в реальному масштабі часу* є одним з актуальних завдань для визначення необхідних параметрів та характеристик захищеності об'єктів інформаційної діяльності та з іншого боку імітації можливостей зловмисників по перехопленню такого роду сигналів.

Порівняння основних технічних характеристик зразків *аналізаторів спектра сигналів* наведено в таблиці 1, що складена авторами з використанням [9; 10; 11; 12]. Для того, щоб моделювати утворення каналу витоку інформації за рахунок ПЕМВН необхідно послідовно описати процеси, які відбуваються за розповсюдження небезпечних інформативних сигналів від джерела їх походження до приймального пристрою зловмисника (аналізатора спектра), і які зводяться до:

розрахунку співвідношення сигнал/шум на вході аналізатора спектра зловмисника за заданих умов;

моделювання процесу перетворення прийнятого вхідного сигналу аналізатором спектра зловмисника;

отримання інформаційного критерія (показника), який визначає ефективність роботи приймального пристрою зловмисника (аналізатора спектра) в процесі добування інформації.

Основні технічні характеристики аналізаторів спектра сигналів реального часу [9; 10; 11; 12]

Параметри	Аналізатори спектра сигналів			
	Anritsu MS2850A (Японія, США) [9]	Rigol RSA3045 (Китай) [10]	Tektronix RSA513A (США) [11]	Aaronia SPECTRAN V6 ECO (Німеччина) [12]
Діапазон робочих частот приймального пристрою ΔF ,	9 кГц ... 32ГГц	9 кГц ... 4,5 ГГц	9 кГц ... 7,5 ГГц	9 кГц... 18 ГГц
Ширина смуги захоплення для аналізу сигналів Δf , Гц	255 МГц, (510 МГц, 1 000 МГц)	10 МГц (25 МГц, 40 МГц опц.)	10, 20, 40 МГц	44 МГц, 60 МГц
Рівень власних шумів приймального пристрою DANL, дБм	-142 дБм/Гц	-161 дБм/Гц	-160 дБм/Гц	-170 дБм/Гц.
Крок перебудови частоти SPAN, МГц	до 30 МГц	10, 25, 40 МГц	10, 20, 40 МГц	н.д.
Гарантоване захоплення сигналів з мінімальною тривалістю, t	н.д.	9,3 мкс	до 100 мкс.	н.д.
Амплітуда, U	від +30 дБм до -166 дБм.	від +30 дБм до -141 дБм.	від +30 дБм до -160 дБм.	від +23 дБм до -170 дБм
Роздільна здатність, (RBW)	1 Гц ... 10 МГц.	200 Гц, 9 кГц, 120 кГц, 1 МГц		62 МГц до 200 МГц
Інтерфейси	USB, Ethernet, IEEE-488 (GPIB).	USB, LAN, HDMI	USB	н.д.
Максимальна частота дискретизації	н.д.	51,2 Мвб / сек	н.д.	н.д.

Стосовно технічного каналу витоку інформації за рахунок ПЕМВН, його структурна схема є сукупністю джерела інформації, середовища поширення інформативних сигналів з урахуванням

впливу зовнішніх шумів і завад та розвідувального приймача зловмисника з відповідними характеристиками (рис. 1).

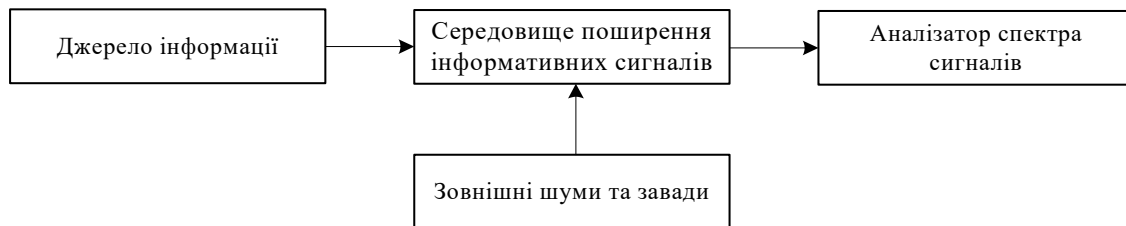


Рисунок 1 – Узагальнена структурна схема виявлення побічних електромагнітних випромінювань та наведень за допомогою аналізатора спектра сигналів

Основними характеристиками джерела інформації, які суттєво впливають на можливості добування інформації зловмисником можна віднести: потужність випромінювання P_{Σ} , несуча частота сигналу f , ширина спектру сигналу Δf , висота підйому антени над рівнем моря, коефіцієнт спрямованої дії антени $G_{апп}$, коефіцієнт бічних пелюсток антени K_{δ} .

До основних характеристик середовища поширення небезпечних сигналів (ПЕМВН), що

істотно впливають на можливості добування інформації зловмисником належать: дальність між джерелом інформації та приймальним пристроєм зловмисника, яка визначається їхніми координатами, виконанням умови прямої видимості, а також протяжністю ділянок, на яких сигнал поширюється в атмосфері та завади.

Що стосується основних характеристик приймального пристрою зловмисника, які істотно впливають на можливості добування ним інформації, можна віднести такі: чутливість приймача, під якою розуміють мінімальну

потужність на вході приймального пристрою зловмисника, за якої здійснюється прийом сигналів із заданою якістю; висота підйому антени над рівнем моря; коефіцієнт спрямованої дії антени приймача; діапазон робочих частот приймального пристрою, ширина смуги перепускання високочастотного і смугового фільтрів приймального пристрою; рівень шумів приймального пристрою, який вимірюється при смузі перепускання приймача $\Delta F = 1$ Гц; крок перебудови частоти або швидкість сканування в реальному масштабі часу.

Для моделювання каналу витоку інформації за рахунок ПЕМВН доцільно використати теорію виявлення та розпізнавання сигналів. А в якості показника ефективності роботи аналізатора спектра сигналів використаємо енергетичний критерій.

З метою отримання співвідношення сигнал/шум на вході аналізатора спектра зловмисника для каналу витоку інформації за рахунок ПЕМВН проведемо моделювання виходячи з таких міркувань. Під час поширення радіохвиль у вільному просторі щільність потоку потужності від ізотропного випромінювача на дальності D визначається виразом [13]:

$$S_{\text{п.п.}} = \frac{P_{\Sigma}}{4\pi D^2},$$

де P_{Σ} – потужність джерел ПЕМВН, Вт;

$4\pi D^2$ – площа сфери радіуса D , яка апроксимує фронт електромагнітної хвилі з рівномірним розповсюдженням;

D – відстань від джерел ПЕМВН до аналізатора спектра зловмисника.

Якщо джерелом випромінювання ПЕМВН є випадкові антени, що утворені елементами конструкції технічного засобу обробки інформації та характеризуються коефіцієнтом підсилення $G_{\text{вип. ант.}}$, то щільність струму потужності на відстані D в напрямку максимуму випромінювання буде в G раз більше, ніж у випадку ізотропного джерела тої самої потужності, тобто:

$$S_{\text{п.п.}} = \frac{P_{\Sigma} G_{\text{вип. ант.}}}{4\pi D^2}, \quad (1)$$

де $G_{\text{вип. ант.}}$ – коефіцієнт спрямованої дії випадкових антен, що утворені елементами конструкції технічного засобу обробки інформації.

За відомої ефективної площі приймальної антени засобу розвідки A потужність сигналу на вході приймальної антени буде дорівнювати:

$$P_{\text{прм}} = A \cdot S_{\text{п.п.}}$$

Коефіцієнт підсилення приймальної антени $G_{\text{прм}}$ та ефективна площа розсіювання приймальної антени A (розкриті антени, рахується розташованим нормально до вектору Умова-Пойнтінга) зв'язані співвідношенням:

$$A = \frac{\lambda^2 G_{\text{прм}}}{4\pi}, \quad (2)$$

де λ – довжина хвилі випромінювання, м.

З урахуванням (1) формулу (2) запишемо у вигляді:

$$P_{\text{прм}} = \frac{\lambda^2 G_{\text{прм}}}{4\pi} \cdot \frac{P_{\Sigma} G_{\text{вип. ант.}}}{4\pi D^2} \quad (3)$$

У реальних умовах поширення радіохвиль втрати енергії можуть зрости не тільки зі збільшенням відстані через сферичну розбіжність фронту хвилі, а й через поглинання і розсіювання електромагнітної енергії в земній поверхні, іоносфері, а також через просторовий перерозподіл енергії під час інтерференції хвиль. Тому, в формулу (3) додамо множники:

$10^{-0.1\alpha D}$ – який враховує згасання ПЕМВН в атмосфері, де α – коефіцієнт згасання ПЕМВН в атмосфері;

γ – коефіцієнт, який враховує розбіжність поляризації ПЕМВН та поляризації приймальної антени аналізатора спектра;

ψ – коефіцієнт передачі потужності вхідного сигналу (ПЕМВН) з виходу антени до входу аналізатора спектра, який залежить від ККД фідерного тракту і виконання умов його узгодження з навантаженням;

K_f – коефіцієнт використання спектральної щільності ПЕМВН $S_{\text{п.п.}}(f)$;

$$K_f = \frac{\Delta f_{\text{прм}}}{\Delta F_{\text{пемвн}}}$$

$$P_{\text{прм}} = \frac{\lambda^2 G_{\text{прм}}}{4\pi} \cdot \frac{P_{\Sigma} G_{\text{вип. ант.}}}{4\pi D^2} \cdot \gamma \cdot \psi \cdot K_f \quad (4)$$

Зробимо декілька зауважень відповідно співвідношення (4). Зауваження 1. ПЕМВН носять всеспрямований характер, це дає змогу прийняти $G_{\text{вип. ант.}} \approx 1$.

Зауваження 2. Апроксимуючи амплітудно-частотну характеристику приймача аналізатора спектра та спектральну щільність ПЕМВН прямокутними функціями, див рис. 2, отримаємо наступне:

$$K_f = \frac{\Delta f_{\text{прм}}}{\Delta F_{\text{пемвн}}}, \text{ при } \Delta F_{\text{пемвн}} \geq \Delta f_{\text{прм}}, \text{ та}$$

$$K_f = 1, \text{ при } \Delta F_{\text{пемвн}} < \Delta f_{\text{прм}}$$

Зауваження 3. Будемо вважати, що ψ – коефіцієнт передачі потужності вхідного сигналу (ПЕМВН) з виходу антени до входу аналізатора спектра дорівнює одиниці. Тобто виконується умова узгодження вихідного опору антени з вхідними опором аналізатора спектра і тоді коефіцієнт передачі потужності вхідного сигналу (ПЕМВН) з виходу антени до входу аналізатора спектра в виразі (4) дорівнює одиниці.

$$\psi = 1$$

Зауваження 4. Будемо вважати, що поляризація ПЕМВН та поляризація приймальної антени аналізатора спектра співпадають, тоді коефіцієнт γ у виразі (4) дорівнює одиниці.

$$\gamma = 1$$

Зауваження 5. Умови, відмінні від умов викладених у зауваженнях 3 та 4, буде розглянуто у подальших публікаціях.

Потужність сигналу на вході лінійної частини приймача можна розрахувати за формулою:

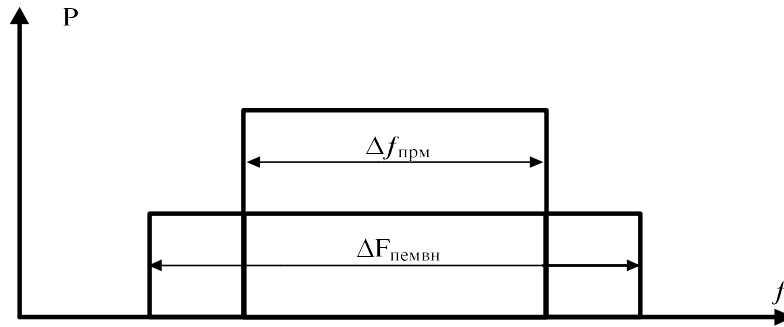


Рисунок 2 – До розрахунку коефіцієнта використання спектральної щільності побічних електромагнітних випромінювань і наведень, K_f

$$\frac{P_{\Sigma}}{P_{\text{прм}}} = \frac{16\pi^2 D^2 \Delta F_{\text{пемвн}}}{\lambda^2 G_{\text{прм}} G_{\text{вип. ант.}} \Delta f_{\text{прм}}}$$

Враховуючи, що чутливість аналізатора спектра $P_{\text{прм min}}$ в основному визначається рівнем його внутрішніх шумів, тоді відношення сигнал/шум визначатиметься так:

$$q = \frac{P_{\Sigma}}{P_{\text{прм min}}} = \frac{16\pi^2 D^2 \Delta F_{\text{пемвн}}}{\lambda^2 G_{\text{прм}} G_{\text{вип. ант.}} \Delta f_{\text{прм}}} \quad (5)$$

Результат ефективності аналізатора спектру прямо пропорційна добутку енергії сигналу на вході аналізатора спектру та відстані між джерелом ПЕМВН та аналізатором спектру, і зворотно-пропорційна добутку довжини хвиль випромінювання, коефіцієнтів спрямованої дії антени аналізатору спектру, коефіцієнтів спрямованої дії випадкових антени – джерел ПЕМВН та ширини смуги перепускання аналізатора спектру.

Для подальшого моделювання процесів, що відбуваються в технічному каналі витoku інформації за рахунок ПЕМВН, необхідно розробити модель прийнятого аналізатором спектру вхідного сигналу. Вона, являє собою сукупність ПЕМВН, які утворені конструктивними елементами технічного засобу, та можуть відігравати роль випадкових антен. Такі сигнали можна представити у вигляді щільності розподілу амплітуд сигналів, що схильні до випадкових флуктуацій. Водночас, достатньо повно статистичні властивості сигналів можуть бути описані законом розподілу та спектром флуктуацій або кореляційною функцією.

В теорії гармонічного аналізу випадкових процесів той факт, що кореляційна функція та спектральна щільність складають пару перетворення Фур'є, відомий як теорема Вінера-Хінчина.

Оскільки сигнали ПЕМВН мають складний характер та схильні до випадкових флуктуацій, їх слід характеризувати, користуючись методами теорії ймовірності. За таких умов, досить повно статистичні властивості сигналів можуть бути

описані законами розподілу і спектром флуктуацій або кореляційною функцією.

Припустимо, що сукупний сигнал джерела ПЕМВН має складний характер та складається з великої кількості вільним чином орієнтованих випадкових антен у складі досліджуваного технічного засобу. Разом із тим, у складі цього сигналу є елементи, що обумовлюють стабільний сигнал (тактова частота роботи технічного засобу що досліджується), амплітуда якого може перевищувати суму амплітуд сигналів, сформованих всіма іншими елементами. На відміну від даної складової сигналу, амплітуди і фази сигналів сформованих випадковими антенами технічного засобу що досліджується зазнають випадкових змін під час його роботи. Така ситуація подібна до тої коли під час спостереження поодиноких об'єктів, які інтенсивно та стабільно відбивають сигнал, на тлі просторово-розподіленої цілі (дипольні завади, тощо) або коли в складі складної цілі є елемент, що інтенсивно і стабільно відбиває [13].

$$u = U_0 \cos \omega t + \sum_{i=1}^n U_i \cos(\omega t - \varphi_i)$$

де U_0 – амплітуда сигналу ПЕМВН що дає стабільний сигнал (тактова частота роботи технічного засобу що досліджується);

U_i – амплітуда сигналу i -го елемента (i -тої випадкової антени), φ_i – фазовий зсув сигналу i -го елемента (i -тої випадкової антени). Якщо результуючу амплітуду суми випадкових елементарних сигналів позначити через U_{Σ} , а фазу – φ_{Σ} , то записаний нами вираз прийме вигляд:

$$u = U_0 \cos \omega t + U_{\Sigma} \cos(\omega t - \varphi_{\Sigma})$$

Розкладемо коливання $u_{\Sigma} = U_{\Sigma} \cos(\omega t - \varphi_{\Sigma})$ на дві ортогональні складові, з котрих косинусоїдальна складова співпадає по фазі зі стабільним сигналом (який обумовлений тактовою частотою роботи технічного засобу, що досліджується).

$$u_{\Sigma} = U_{\Sigma 1} \cos \omega t + U_{\Sigma 2} \sin \omega t,$$

де $U_{\Sigma 1} = U_{\Sigma} \cos \varphi_{\Sigma} = \sum_{i=1}^n U_i \cos \varphi_i$;

$$U_{\Sigma 2} = U_{\Sigma} \sin \varphi_{\Sigma} = \sum_{i=1}^n U_i \sin \varphi_i.$$

$$U_{\Sigma} = \sqrt{U_{\Sigma 1}^2 + U_{\Sigma 2}^2}; \quad \text{tg } \varphi_{\Sigma} = U_{\Sigma 2} / U_{\Sigma 1}$$

Косинусоїдальна складова випадкового сигналу разом з співпадаючим за фазою постійним за величиною сигналом дає результуючий вектор $U_1 = U_0 + U_{\Sigma 1}$, а синусоїдальна складова випадкового сигналу представляє собою вектор $U_2 = U_{\Sigma 2}$, який ортогональний вектору U_1 . Вочевидь, що амплітуди ортогональних складових U_1 та U_2 є незалежними величинами – зміна однієї не впливає на зміну іншої.

Вектор U , який дорівнює геометричній сумі ортогональних складових U_1 та U_2 , представляє собою результуючий сигнал амплітуда та фаза якого є випадковими величинами:

$$u = U \cos(\omega t - \varphi) = U_0 \cos \omega_0 t + U_{\Sigma} \cos(\omega t - \varphi_{\Sigma})$$

Під час зміни положення аналізатора спектру сигналів відносного джерела ПЕМВН, будуть змінюватись відстані до елементарних випромінювачів (випадкових антен), як наслідок будуть змінюватись фазові співвідношення між сигналами, що вони випромінюють. Це призведе до випадкової зміни амплітуд та фаз сигналів ПЕМВН. Внаслідок чого будуть випадковим чином змінюватись і амплітуди складових $U_{\Sigma 1}$ та $U_{\Sigma 2}$. Через те, що кожна з цих складових є результатом поєднання великої кількості сигналів, утворених елементарними випадковими антенами технічного засобу, що досліджується, для яких справедлива центральна гранична теорема теорії імовірності. Тому будемо вважати, що амплітуди випадкових ортогональних складових $U_{\Sigma 1}$ та $U_{\Sigma 2}$ підпорядковуються нормальному закону розподілу

$$W(U_{\Sigma 1}) = (1/\sqrt{2\pi} \sigma_1) \exp(-U_{\Sigma 1}^2/2\sigma_1^2),$$

$$W(U_{\Sigma 2}) = (1/\sqrt{2\pi} \sigma_2) \exp(-U_{\Sigma 2}^2/2\sigma_2^2),$$

де $\sigma_1^2 = U_{\Sigma 1}^2$ та $\sigma_2^2 = U_{\Sigma 2}^2$ – дисперсія амплітуд ортогональних складових.

З урахуванням фізичної симетрії розкладення випадкової результуючої напруги на ортогональні складові можна стверджувати, що $\sigma_1^2 = \sigma_2^2 = \sigma^2$. Знаючи закони розподілу випадкових амплітуд $U_{\Sigma 1}$ та $U_{\Sigma 2}$, можна визначити закони розподілу амплітуд ортогональних складових U_1 та U_2 , середні значення яких $\overline{U_1} = \overline{U_0}$, $\overline{U_2} = 0$. Самі величини U_1 та U_2 випадково коливаються відносно своїх середніх значень, які підкоряються нормальному закону розподілу:

$$W(U_1) = (1/\sqrt{2\pi} \sigma) \exp[-(U_1 - U_0)^2/2\sigma^2],$$

$$W(U_2) = (1/\sqrt{2\pi} \sigma) \exp[-U_2^2/2\sigma^2].$$

Водночас, ортогональні складові U_1 та U_2 також статистично незалежні. В таких умовах, як відомо, амплітуда результуючого сигналу $U = \sqrt{U_1^2 + U_2^2}$ є випадковою величиною, щільність імовірності якої підпорядковується узагальненому закону Релея:

$$W(U) =$$

$$= (U/\sigma^2) \exp[-(U^2 + U_0^2)/2\sigma^2] I_0(UU_0/\sigma^2) \quad (6)$$

де I_0 – функція Бесселя першого роду нульового порядку від уявного аргументу. При відсутності

стабільної складової сигналу $U_0 = 0$ та $I_0(UU_0/\sigma^2) = I_0(0) = 1$.

Внаслідок цього, щільність імовірності результуючої амплітуди сигналів випадкових антен буде визначатися законом Релея:

$$W(U) = (U/\sigma^2) \exp(-U^2/2\sigma^2) \quad (7)$$

Розподіли (6) та (7) можливо записати в більш загальному вигляді, якщо ввести відносні величини:

$$a = \frac{U_0}{\sigma}, \quad v = \frac{U}{\sigma},$$

Тоді після перетворень від розподілів (6) і (7) переходимо до розподілів для відносної величини:

$$W(v) = v \exp[-(v^2 + a^2)/2] I_0(av), \quad (8)$$

$$W(v) = v \exp(-v^2/2). \quad (9)$$

За відсутності стабільної складової сумарний сигнал утворюється в результаті додавання тільки сигналів випадкових відбивачів. Математичне очікування відносної амплітуди цього сигналу:

$$\bar{v} = \int_0^{\infty} v \exp(-v^2/2) dv = \sqrt{\pi/2},$$

а дисперсія відносної амплітуди:

$$\overline{(v - \bar{v})^2} = (4 - \pi)/2$$

Отже, *отримана формалізована модель виявлення та оцінки ПЕМВН на об'єктах інформаційної діяльності за енергетичним критерієм містить в собі, переважно, всі основні фізичні характеристики приймача. Ці характеристики суттєво визначають узагальнену чутливість та ефективність роботи апаратних або апаратно-програмних комплексів, побудованих на основі аналізаторів спектра сигналів. Пороговий рівень P_{\min} , що визначає мінімальну чутливість аналізатора спектру та прямо пропорційно залежить від енергії сигналу на вході аналізатора спектру, довжини хвиль випромінювання, коефіцієнтів спрямованої дії антени аналізатору спектра, коефіцієнтів спрямованої дії випадкових антени – джерел ПЕМВН та ширини смуги перепускання аналізатора спектру, та зворотньо пропорційний відстані між джерелом ПЕМВН та аналізатором спектра і шириною спектру сигналу ПЕМВН.*

Вираз (5) дає змогу прогнозувати параметри аналізатора спектра сигналів, що розробляються або вже існуючих моделей на основі характеристик приймача. І навпаки, він дозволяє правильно вибрати тип аналізатора спектру для виявлення прогнозованих параметрів сигналів ПЕМВН.

Наукова новизна описаних пропозицій полягає в їхній комбінації та спрямованості на покращення ефективності роботи аналізаторів спектру, що можливо досягти за рахунок зниження власних шумів аналізатора спектру та підвищення розрізняльної здатності (розрізнення джерел ПЕМВН за частотою).

Власний шум пристрою, розглянутого вище, визначався шумовими характеристиками

мікросхеми підсилювача і шириною частотного діапазону вимірювання. Звідси випливає, що зменшення частотної смуги призведе до зменшення власного шуму детектора. Це завдання розв'язується шляхом використання групи смугових фільтрів, що перекривають частотний діапазон, який цікавить. Збільшення числа фільтрів призводить до поліпшення співвідношення сигнал/шум.

Крім того, ці ж фільтри дають змогу підвищити розрізняльну здатність аналізатора спектру за частотою. У результаті цього у аналізатора спектру сигналів з'являється здатність виявляти дуже слабкі джерела електромагнітного випромінювання на тлі дуже сильних, що абсолютно неможливо для широкопсмугового детектора.

Розроблені пропозиції з удосконалення технічних характеристик аналізаторів спектра сигналів дають змогу досягти максимального результату виявлення та розпізнавання інформативних сигналів від джерел ПЕМВН, що можуть бути використані на ОІД.

Висновки й перспективи подальших досліджень

У статті, на основі математичної моделі технічного каналу витоку інформації, за рахунок побічних електромагнітних випромінювань і наведень розроблено пропозиції з удосконалення технічних характеристик аналізаторів спектра сигналів, а саме:

зниження власних шумів;
підвищення розрізняльної здатності (розрізнення джерел побічних електромагнітних випромінювань та наведень за частотою).

Ці пропозиції підвищують якість виявлення та ідентифікацію джерел електромагнітних випромінювань з метою подальшої нейтралізації радіоелектронних засобів несанкціонованого знімання інформації, що можуть бути впроваджені на об'єкті інформаційної діяльності в сучасних умовах. А також – надавати рекомендації щодо розташування обладнання на об'єкті інформаційної діяльності з метою недопущення впливу побічних

Список бібліографічних посилань

1. Травніков Є. М., Лазебний В. С., Власюк Г. Г., Пілінський В. В., Співак В. М., Швайченко В. Б. Конструювання та технологія виробництва техніки реєстрації інформації: У 3-х кн. Кн. 2. Основи конструювання. Навчальний посібник. Київ : «Кафедра», 2015. 285 с. URL: <https://ela.kpi.ua/handle/123456789/18959> (дата звернення: 26.06.2024). 2. Wim Van Eck. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security*. Author links open overlay panel Wim van Eck. 1985. Vol. 4. Is. 4, P. 269–286. URL: <https://www.sciencedirect.com/science/article/> (Accessed: 12 May 2024). 3. Kuhn M. G. Compromising emanations: eavesdropping risks of computer displays. This technical report is based on a dissertation submitted June 2002 by the author for the degree of Doctor of Philosophy to the University of Cambridge, Wolfson College. Technical reports published by the University of Cambridge Computer

електромагнітних випромінювань і наведень на інше обладнання об'єкту інформаційної діяльності та створення технічних каналів витоку інформації. Подані рекомендації спрямовані на покращення ефективності використання аналізаторів спектру сигналів у виявленні та захисті від потенційних загроз, що походять із засобів обробки інформації. Застосування запропонованих технічних рішень може виявитися критичним у забезпеченні безпеки та конфіденційності на об'єктах інформаційної діяльності в умовах сучасних технологічних викликів.

Практичною цінністю результатів дослідження є підвищення якості виявлення, оцінки та нейтралізації побічних електромагнітних випромінювань і наведень, джерелами яких можуть бути радіоелектронні засоби й системи обробки та передачі інформації, що розташовані на об'єкті інформаційної діяльності, шляхом покращення енергетичного критерію роботи аналізаторів спектра сигналів.

Отже, мета статті, що зводиться до розроблення пропозицій з удосконалення технічних характеристик аналізаторів спектра сигналів для виявлення та оцінки побічних електромагнітних випромінювань і наведень, які потенційно можуть бути сформовані технічними засобами обробки інформації на об'єкті інформаційної діяльності, досягнута.

Напрямами подальших досліджень слід вважати удосконалення вбудованих алгоритмів для автоматичного виявлення та аналізу побічних електромагнітних випромінювань і наведень, що дасть змогу користувачам ефективно використовувати аналізатори спектра сигналів в апаратно-програмних комплексах для створення систем мультисенсорної обробки даних, а також створення додатків та інтерфейсів для мобільних пристроїв, що дозволить в реальному масштабі часу вести контроль електромагнітних випромінювань на визначених об'єктах, виявляти, аналізувати та оцінювати параметри побічних електромагнітних випромінювань і наведень.

Laboratory are freely available via the Internet, 2003. URL: <http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-577.pdf>. (Accessed: 27 March 2024). 4. Smulders P. The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables. *Computers & Security*. 1990. Vol. 9. P. 53–58. URL: <https://www.sciencedirect.com/science/article/abs/pii/0167404890901570> (Accessed: 30 March 2024). 5. Vuagnoux M., Pasini S. Compromising Electromagnetic Emanations of Wired and Wireless Keyboards, *18th USENIX Security Symposium (Usenix Security '09)*, Montreal, Canada, August 10-14, 2009. P. 1–16. URL: <https://dl.acm.org/doi/10.5555/1855768.1855769> (Accessed: 03 May 2024). 6. Kuhn M G. Electromagnetic Eavesdropping Risks of Flat-Panel Displays, *4th Workshop on Privacy Enhancing Technologies*, 26-28, Toronto, Canada, Proceedings, LNCS 3424. 2009. P. 88–105, Springer-Verlag. URL: <https://www.researchgate.net/>

publication/2873011_Electromagnetic_Eavesdropping_Risks_of_Flat-Panel_Displays (Accessed: 30 April 2024).
 7. Юли-Мяюрн В., Мнята Д., Хомма Н., Аоки Т., Хаяси Ю. Об оценке утечки электромагнитной информации с экранов мобильных устройств. *Международный симпозиум IEEE по электромагнитной совместимости 2018 г. и Азиатско-Тихоокеанский симпозиум IEEE по электромагнитной совместимости 2018 г., EMC/APEMC. 2018*, 1050-1052. URL: <https://ieeexplore.ieee.org/document/8393945> (Accessed: 18.05.2024).
 8. Maxwell M. A Tempest vulnerability prediction method for cyber security practitioners. *Alexandria Engineering Journal*. 2023. Vol. 78. P. 561–575. URL: <https://www.sciencedirect.com/science/article/pii/S111001682300652X> (Accessed: 24 April 2024).
 9. Серія аналізаторів до 44,5 ГГц із смугою аналізу до 1 ГГц Anritsu MS2850A. 2024. URL: <https://www.tehcom.com/Companies/Anritsu/MS2850A/>

Anritsu_MS2850A-047-046-u.htm (дата звернення: 16.05.2024).
 10. Аналізатор спектра реального часу Rigol RSA3045. 2024. URL: <https://metranom.com/product/analizator-spektra-realnogo-vremeni-rigol-rsa3045/> (дата звернення: 18.05.2024).
 11. Серія аналізаторів спектру, кабелів та антен до 18 ГГц Tektronix RSA500A. 2024. URL: https://www.tehcom.com/Companies/Tektronix/RSA500A/Tektronix_RSA500A_RSA503A_RSA507A-u.htm (дата звернення: 19.05.2024).
 12. USB аналізатор спектру Aaronia SPECTRAN V6 ECO 150XA-18 до 18 ГГц. 2024. URL: <https://www.tehcom.com/analizatory-spektru/aaronia-spectran-v6-eco-150xa-18-usb-analizator-spektru> (дата звернення: 21.05.2024).
 13. Коростылев А. А., Ключев Н. Ф., Мельник Ю. А. Теоретические основы радиолокации : Навчальний посібник. 2-е вид., перероб. та доп., 1978, 608 с.

PROPOSALS FOR IMPROVING THE TECHNICAL CHARACTERISTICS OF SIGNAL SPECTRUM ANALYSERS

Konotopets Mykola (Candidate of Technical Sciences, Associate Professor)¹

Samoilov Ihor (Candidate of Technical Science, Associate Professor)¹

Storchak Anton (Candidate of Technical Science)¹

Smolkov Oleksandr (Candidate of Technical Science)²

¹*Institute of Special Communications and Information Protection National Technical University of Ukraine*

«Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine

²*National Defence University of Ukraine, Kyiv, Ukraine*

Formulation of the problem in general. The purpose of the article is to develop proposals for improving the technical characteristics of signal spectrum analyzers for the detection, evaluation and analysis of electromagnetic fields that arise during the operation of technical means of information processing at the objects of information activity and can serve as a source of information for criminals.

Research methods. The presented mathematical apparatus made it possible to analyse the mathematical dependencies of the parameters of detection of dangerous signals by signal spectrum analysers based on the characteristics of the receiver. The synthesis method was used to develop proposals for improving the technical characteristics of signal spectrum analysers. Also, using technical and technological methods for detecting and assessing side electromagnetic radiation and interference that may arise in the process of operation of radio electronic means of processing, storing and exchanging information at information facilities, a model for detecting side electromagnetic radiation and interference of dangerous signals by the energy criterion, which includes the main physical characteristics of the receiver, was formalised.

Analysis of recent researches and publications. The results of the study of the possibility of extracting information from video displays by intercepting and decoding unintentional electromagnetic radiation and interference generated by this type of equipment during their operation are presented. The problems of intercepting side electromagnetic radiation and interference of video monitors with VGA and DVI interfaces are investigated. The methodology for assessing the electromagnetic radiation and interference of the mobile device under test is presented. The validity of the presented methodology is demonstrated in real conditions by an experiment on monitoring the electromagnetic radiation of the tablet screen, which can be used in the TEMPEST attack. Given the above, the study on improving the quality of detection and neutralisation of side electromagnetic radiation and interference arising in the process of operation of technical means of information processing that can be used at information facilities in modern conditions is an urgent scientific task.

Presenting the main material. The article develops proposals for improving the technical characteristics of a signal spectrum analyser for detecting and assessing EMPs. Being part of hardware or hardware-software complexes designed to solve the problems of instrumental control, signal spectrum analysers detect, evaluate (measure) and analyse the spatial-frequency characteristics of hazardous signals arising in the process of operation of radioelectronic information processing equipment at information facilities. Such signals, in turn, can characterise sources of electromagnetic radiation and interference and be considered as a component of potential technical channels of information leakage. A formalised model for detecting EMI at information activity objects according to the energy criterion has been developed on the basis of the theory of signal detection and recognition with consideration of external and internal noise.

Elements of scientific novelty. The scientific novelty of the work is the specification of the known data and their extension to new objects of research, which are own side electromagnetic radiation and guidance of radio electronic information processing equipment that can be used at the objects of information activity.

Theoretical and practical significance of the article. The value of the obtained research results in the military and technical fields is to gain knowledge about the possibilities of improving the quality characteristics of radio wave monitoring equipment and a certain sequence of actions to prevent the interception of information by intruders. These results can be used at the objects of information activity in modern conditions.

Conclusion and the perspectives of future researches. In the article, on the basis of the mathematical model of the technical channel of information leakage due to unintentional electromagnetic radiation and guidance, proposals for improving the technical characteristics of signal spectrum analysers are developed, namely: reduction of intrinsic noise; increase of the resolution (distinguishing electromagnetic pulse sources by frequency). These proposals improve the quality of detection and neutralisation of radioelectronic means of information acquisition that can be used on the object of information activity in modern conditions. Areas for further research should include improving built-in algorithms for automatic detection and analysis of side electromagnetic radiation and interference, which will allow users to effectively use signal spectrum analysers in hardware and software systems to create multisensor data processing systems, as well as create applications and interfaces for mobile devices, which will allow real-time radio monitoring, detection, analysis and evaluation parameters of unintentional electromagnetic radiation and guidance.

Keywords: electronic equipment, radio electronic information processing equipment, signal spectrum analyser, amplitude-frequency response, dangerous signal, technical channels of information leakage, radio wave control, hardware, hardware and software complex, radiation pattern.

References

1. Travnikov, E. M., Lazebnyi, V. S., Vlasiuk, G. G., Pilinskyi, V. V., Spivak, V. M., Shvaichenko, V. B., (2015). *Design and production technology of information recording equipment*: In 3 books. Book 2. Fundamentals of design. Study guide. Kyiv: «Kafedra» [online]. Available at: <https://ela.kpi.ua/handle/123456789/18959> [Accessed: 26 June 2024].
2. Wim van Eck, (1985). Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security* [online]. Author links open overlay panel Wim van Eck. 4, 4. Available at: <https://www.sciencedirect.com/science/article/> [Accessed: 12 May 2024].
3. Kuhn, M. G., (2003). Compromising emanations: eavesdropping risks of computer displays. This technical report is based on a dissertation submitted June 2002 by the author for the degree of Doctor of Philosophy to the University of Cambridge, Wolfson College. Technical reports published by the University of Cambridge Computer Laboratory are freely available via the Internet [online]. Available at: <http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-577.pdf> [Accessed: 27 March 2024].
4. Smulders, P., (1990). The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables. *Computers & Security*, 9, 53–58 [online]. Available at: <https://www.sciencedirect.com/science/article/abs/pii/0167404890901570> [Accessed: 30 March 2024].
5. Vuagnoux, M., Pasini, S., (2009). Compromising Electromagnetic Emanations of Wired and Wireless Keyboards, 18th USENIX Security Symposium (Usenix Security '09), Montreal, Canada, August 10-14, 1-16 [online]. Available at: <https://dl.acm.org/doi/10.5555/1855768.1855769> [Accessed: 3 May 2024].
6. Kuhn, M. G., (2004). Electromagnetic Eavesdropping Risks of Flat-Panel Displays, 4th Workshop on Privacy Enhancing Technologies, 26-28, Toronto, Canada, Proceedings, LNCS 3424, 88–105, Springer-Verlag [online]. Available at: https://www.researchgate.net/publication/2873011_Electromagnetic_Eavesdropping_Risks_of_Flat-Panel_Displays [Accessed: 30 April 2024].
7. Yli-Mayry, V., Miyata, D., Homma, N., Aoki, T., Hayashi, Y., (2018). On the evaluation of electromagnetic information leakage from mobile device screens. *IEEE International Symposium on Electromagnetic Compatibility 2018 and IEEE Asia-Pacific Symposium on Electromagnetic Compatibility 2018, EMC/APEMC 2018*, 1050-1052, [online]. Available at: <https://ieeexplore.ieee.org/document/8393945> [Accessed: 18 May 2024].
8. Martin, M., (2023). A Tempest vulnerability prediction method for cyber security practitioners. *Alexandria Engineering Journal*. 78, 561-575, [online]. Available at: <https://www.sciencedirect.com/science/article/pii/S111001682300652X> [Accessed: 24.04.2024].
9. Anritsu MS2850A series of analyzers up to 44.5 GHz with an analysis bandwidth up to 1 GHz [online], (2024). Available at: https://www.tehcom.com/Companies/Anritsu/MS2850A/Anritsu_MS2850A-047-046-u.htm [Accessed: 16 May 2024].
10. Real-time spectrum analyzer Rigol RSA3045 [online], (2024). Available at: <https://metranom.com/product/analizator-spektra-realnogo-vremeni-rigol-rsa3045/> [Accessed: 18 May 2024].
11. Tektronix RSA500A series of spectrum analyzers, cables and antennas up to 18 GHz [online], (2024). Available at: https://www.tehcom.com/Companies/Tektronix/RSA500A/Tektronix_RSA500A_RS_A503A_RSA507A-u.htm [Accessed: 19 May 2024].
12. USB spectrum analyzer Aaronia SPECTRAN V6 ECO 150XA-18 up to 18 GHz [online], (2024). Available at: <https://www.tehcom.com/analizatory-spektru/aaronia-spectran-v6-eco-150xa-18-usb-nalizator-spektru> [Accessed: 21 May 2024].
13. Korostylev, A. A., Klyuev, N. F., Melnik, Y. A., (1978). *Theoretical bases of radiolocation*. Study guide. 2nd ed., revised and supplemented.