© Humeniuk I., Zaviriukha D., Kosterev D., Lahodnyi O., Sheihas V. Methodology for optimizing the selection of information protecting means from leakage by Transient Electromagnetic Pulse Emanation Standard // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 23-29. © This is an open access article under the CC BY 4.0 International license.*

DOI: 10.18372/2225-5036.32.21654

МЕТОДИКА ОПТИМІЗАЦІЇ ВИБОРУ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ПОБІЧНИМИ ЕЛЕКТРОМАГНІТНИМИ ВИПРОМІНЮВАННЯМИ

Гуменюк Ігор, Завірюха Дмитро, Костерев Дмитро, Лагодний Олександр, Шейгас Віктор

Житомирський військовий інститут імені С. П. Корольова



ГУМЕНЮК Ігор Володимирович, канд. техн. наук, доц.
Рік та місце народження: 1988 рік, смт. Іванопіль, Житомирська обл., Україна.
Освіта: Житомирський військовий інститут імені С. П. Корольова Національного авіаційного університету, 2010 рік.
Посада: професор кафедри охорони державної таємниці та захисту інформації.
Наукові інтереси: методи і засоби захисту інформації, кібербезпека, технічний захист інформації, комп'ютерні мережі та компоненти.
Публікації: понад 90 наукових публікацій, серед яких підручники, патенти на корисні моделі, наукові статті, авторські свідоцтва, тези та матеріали доповідей на конференціях.
E-mail: ig_gum@ukr.net
Orcid ID: 0000-0001-5853-3238



ЗАВІРЮХА Дмитро Олександрович
Рік та місце народження: 1989 рік, с. Вільбівне, Рівненська обл., Україна.
Освіта: Житомирський військовий інститут імені С. П. Корольова Національного авіаційного університету, 2011 рік.
Посада: старший викладач кафедри охорони державної таємниці та захисту інформації.
Наукові інтереси: методи і засоби захисту інформації, протидія технічним розвідкам.
Публікації: більше 10 наукових публікацій, серед яких навчальні та практичні посібники, наукові статті, методичні рекомендації, тези доповідей на конференціях.
E-mail: snigok777@gmail.com
Orcid ID: 0009-0005-6708-8902



КОСТЕРЕВ Дмитро Сергійович
Рік та місце народження: 1987 рік, м. Житомир, Україна.
Освіта: Житомирський військовий інститут імені С. П. Корольова Національного авіаційного університету, 2009 рік.
Посада: старший науковий співробітник науково-дослідного відділу інформаційної та кібернетичної безпеки науково-дослідного управління розвитку спеціальних систем та інновацій.
Наукові інтереси: методи і засоби технічного захисту інформації, технічний захист інформації, протидія технічним розвідкам.
Публікації: понад 30 наукових публікацій, серед яких наукові статті, результати науково-дослідних робіт, тези та матеріали доповідей на конференціях.
E-mail: dima_kos1@ukr.net
Orcid ID: 0000-0002-4076-8386



ЛАГОДНИЙ Олександр Васильович, канд. техн. наук, доц.
Рік та місце народження: 1982 рік, с. Олександрівка, Чернігівська обл., Україна.
Освіта: Житомирський військовий інститут радіоелектроніки імені С. П. Корольова, 2006 рік.
Посада: заступник начальника кафедри охорони державної таємниці та захисту інформації.
Наукові інтереси: методи і засоби технічного захисту інформації, кібербезпека, проєктування систем технічного захисту інформації.
Публікації: понад 60 наукових публікацій, серед яких навчальні посібники, патенти на корисні моделі, наукові статті, авторські свідоцтва, тези доповідей на конференціях.
E-mail: lov.82@ukr.net
Orcid ID: 0000-0002-0812-939X



ШЕЙГАС Віктор Вікторович
Рік та місце народження: 1983 рік, м. Ноябрськ, СРСР.
Освіта: Національний технічний університет України «Київський політехнічний інститут», 2006 рік.
Посада: викладач кафедри охорони державної таємниці та захисту інформації.
Наукові інтереси: протидія технічним розвідкам, технічний захист інформації.
Публікації: більше 20 наукових публікацій, серед яких навчальні посібники, патенти на винаходи, наукові статті, методичні рекомендації, тези доповідей на конференціях.
E-mail: victoryus@i.ua
Orcid ID: 0009-0002-2633-5370

© Humeniuk I., Zaviriukha D., Kosterev D., Lahodnyi O., Sheihas V. Methodology for optimizing the selection of information protecting means from leakage by Transient Electromagnetic Pulse Emanation Standard // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 23-29. © This is an open access article under the CC BY 4.0 International license.*

Анотація. *У роботі обґрунтовано та вирішено важливе науково-практичне завдання, яке полягає в розробленні унікальної методики забезпечення захисту інформації від витоку технічними каналами, що утворюються під час її оброблення відповідними засобами. Необхідність такого завдання обумовлено високим рівнем реалізації загроз інформації цими каналами, а також відсутністю універсального методичного забезпечення щодо впровадження заходів для досягнення необхідного рівня захищеності інформації. Нормативними документами в галузі технічного захисту інформації чітко окреслено процедури аналітичних та вимірювальних робіт щодо визначення показників захищеності інформації та оцінка їх відповідності відповідним нормам. Запропонована методика включає в себе такі кроки: аналіз вихідних даних (частот небезпечних сигналів та інших параметрів на цих частотах), підбір засобів захисту інформації (активного зашумлення), а також оцінювання рівня захищеності інформації за рахунок впроваджених заходів.*

Крім цього, виходячи із аналізу сучасних засобів оброблення інформації, наведеного у роботі, визначено перспективи подальших досліджень щодо необхідності значного розширення частотного діапазону засобів активного електромагнітного зашумлення. Запропонована методика є важливим інструментом для побудови комплексів технічного захисту на об'єктах електронно-обчислювальної техніки.

Ключові слова: *об'єкт електронно-обчислювальної техніки, технічний канал витоку інформації, побічне електромагнітне випромінювання та наведення, захист інформації, небезпечні сигнали, оптимізація.*

Вступ. Інтенсивний розвиток інформаційних технологій, у тому числі, оброблення інформації засобами електронно-обчислювальної техніки (ЕОТ) є одночасною причиною стійкої тенденції щодо удосконалення засобів технічної розвідки (ЗТР), зокрема радіоелектронної. Такий вид розвідки націлений на здобування інформації в результаті приймання й аналізу електромагнітних випромінювань радіодіапазону, створюваних радіоелектронними засобами [1]. Витік інформації та, як наслідок, її перехоплення можливе за рахунок утворення так званих "побічних електромагнітних випромінювань та наведень" (ПЕМВН), утворених під час функціонування основних (ОТЗ) та допоміжних технічних засобів та систем (ДТЗС). У іноземній популярній науково-технічній літературі застосовується термін "compromising emanation" - компрометуюче випромінювання, а також Transient Electromagnetic Pulse Emanation Standard "TEMPEST" – Стандарт випромінювання перехідних електромагнітних імпульсів [2, 3].

Будь-який електронний пристрій, що знаходиться на об'єкті ЕОТ та здійснює оброблення даних, генерує такі побічні електромагнітні випромінювання, які можуть бути перехоплені відповідними ЗТР. Фізичні процеси, що відбуваються у таких пристроях, створюють під час оброблення інформації передумови для появи небезпечних сигналів у навколишньому середовищі, сторонніх інформаційних лініях, ланцюгах електроживлення, заземлення тощо, що створює реальні умови для отримання передбачуваним порушником закритих відомостей, що циркулюють в технічних засобах, за допомогою засобів розвідки. Фізичні явища, що лежать в основі появи небезпечних сигналів за межами контрольованої зони (КЗ), і шляхи їх можливого витоку можуть бути різними. Проте, у загальному вигляді витік інформації може розглядатися як ненавмисне передавання секретної інформації деякою побічною системою зв'язку у вигляді побічних електромагнітних випромінювань. Приймаючи та декодуючи ці випромінювання, порушник може отримати відомості про всю інформацію, що зберігається та обробляється на ЕОТ [4]. Саме тому, захисту інформації від її витоку технічними каналами, утворених за рахунок ПЕМВН, варто приділяти особливої увагу.

Аналіз останніх досліджень і публікацій

На теперішній час проведено низку наукових досліджень вітчизняними та зарубіжними вченими, розроблено достатню кількість наукових праць щодо аналізу, оцінювання рівня ПЕМВН/TEMPEST та шляхів блокування витоку інформації через ці технічні канали. Зокрема, у [2] розглянуто процеси формування технічних каналів витоку інформації на основі високочастотного наведення, а також досліджено спектральний склад та рівні енергії його небезпечних сигналів. Авторами у [4] проведено дослідження електромагнітного екранування як необхідного фізичного заходу для захисту інформації від витоку інформації через побічні електромагнітні випромінювання та наведення, розроблено матеріал для його реалізації та проаналізовано частотно-залежні принципи. У [5] проаналізовано вразливості клавіатур до витоку електромагнітного випромінювання та розроблено спосіб його унеможливлення (блокування) на основі прихованої марковської моделі. У [6] запропоновано методику оцінки захищеності інформації від витоку каналом ПЕМВН засобів ЕОТ при використанні тестового сигналу у вигляді безперервної послідовності імпульсів. Такі підходи можуть бути враховані при вдосконаленні методики проведення спеціальних досліджень (СД) ПЕМВН засобів ЕОТ.

Проте, аналіз досліджень та публікацій свідчить про те, що універсальній методиці щодо забезпечення захисту інформації від витоку ПЕМВН/TEMPEST, яка б включала оцінювання рівня небезпечних сигналів, розрахунок відповідних зон їх поширення, розрахунок відповідних енергетичних та спектральних показників та підбір обладнання щодо блокування (унеможливлення) витоку інформації не присвячено належної уваги.

Саме тому, виходячи з наявних передумов, **метою цієї роботи** є розроблення методики захисту інформації на об'єкті ЕОТ від витоку ПЕМВН.

Виклад основного матеріалу дослідження

Частотний діапазон ПЕМВН, який складає від одиниць кГц до десятків ГГц і вище, визначається тактовою частотою технічного засобу, який приймає участь (допоміжний) або здійснює безпосереднє оброблення (основний) інформації з обмеженим доступом. Якщо раніше нормативні документи в галузі технічного захисту інформації та методики атестації об'єктів інформаційної діяльності (об'єктів

ЕОТ) зосереджувалися переважно на відносно вузькому діапазоні частот відеоінтерфейсів та аналогових дисплеїв (зазвичай до кількох сотень МГц), відтак на теперішній час спектр потенційно небезпечних паразитних випромінювань безпрецедентно розширився (табл. 1–3).

Таблиця 1

Характеристика сучасних операційних процесорів

Модель процесора	Частота ядра, МГц	Частота пам'яті, МГц
GeForce GTX 1050	1354	7000
Intel Celeron	3300	800
Xeon	3800	1600
Intel Core i7	346000	6400
Athlon 64 FX	2000-3200	1000
Sempron	1400-2300	800
Mobile Athlon 64	1600-2600	800
Turion 64	1600-2400	800
Opteron	1700-2500	1000
Phenom II	2500-3400	1800, 2000

Згідно із новітніми дослідженнями каналів витоку інформації, оцінка небезпеки конкретних частот базується не лише на амплітуді ПЕМВН на певній гармоніці, але й на ступені інформативності сигналів, що модулюють ці випромінювання [7].

Варто зазначити, що ПЕМВН утворюються за рахунок небезпечного сигналу, причинами утворення якого є паразитні (шкідливі) зв'язки та наведення. При цьому інформативні сигнали не залежать від ступеня секретності інформації, яка обробляється на об'єкті ЕОТ.

Аналіз ОТЗ, які здійснюють оброблення інформації свідчить про те, що витік інформації можливий на більш високих частотах (до 10-15 гармоніки тактової частоти) порівняно із системами електромагнітного зашумлення (генераторів високочастотного та радіочастотного шуму), які використовуються для зашумлення або подавлення паразитних інформативних випромінювань з діапазоном до 1 ГГц.

Таблиця 2

Характеристика сучасного периферійного обладнання

Модель принтера	Інтерфейси підключення	Частоти / швидкість
HP LaserJet Pro MFP M428fdw	USB 2.0, Ethernet, Wi-Fi	Wi-Fi 2.4 ГГц / Ethernet до 1 Гбіт/с
Brother HL-L8360CDW	USB 2.0, Ethernet, Wi-Fi	Wi-Fi 2.4 ГГц / Ethernet 1 Гбіт
Canon i-SENSYS LBP223dw	USB 2.0, Ethernet, Wi-Fi	Wi-Fi 2.4 ГГц / Ethernet 100 Мбіт
Xerox B235	USB, Ethernet, Wi-Fi	Wi-Fi 2.4 ГГц
Lexmark MB2236adw	USB, Ethernet, Wi-Fi	Wi-Fi 2.4 ГГц / Ethernet 100 Мбіт
Kyocera ECOSYS P2235dn	USB, Ethernet	Ethernet 10/100/1000 Мбіт/с

Таблиця 3

Характеристика носіїв та накопичувачів інформації

Тип носія (накопичувача) інформації	Інтерфейс	Пропускна здатність, МБ/с	Послідовний (послідовне)	
			читання, МБ/с	запис, МБ/s
SSD				
SATA SSD	SATA III (6 Gb/s)	600	450–560	400–530
NVMe PCIe 3.0	PCIe 3.0 x4	3500	2000–3500	1500–3000
NVMe PCIe 4.0	PCIe 4.0 x4	7000	5000–7500	4000–7000
NVMe PCIe 5.0	PCIe 5.0 x4	14000	10000–14500	8000–12000
Зовнішній SSD	USB4 / Thunderbolt 4	4000	2500–3800	2000–3500
HDD				
HDD	SATA III (6 ГБ/с)	600	180–260	150–240
HDD (NAS/Server)	SATA III / SAS	600–1200	200–280	180–260
Enterprise HDD	SAS (12 ГБ/с)	1200	250–350	200–320
Зовнішній HDD	USB 3.0 / 3.2	625–1250	100–180	100–160
Flash-носії та роз'єми				
USB 2.0	USB 2.0	60	10–40	5–25
USB 3.0 / 3.2 Gen1	5 ГБ/с	625	100–250	30–150
USB 3.2 Gen2	10 ГБ/с	1250	300–600	150–400
USB 3.2 Gen2x2	20 ГБ/с	2500	800–2000	500–1500
USB4 / Thunderbolt	20–40 ГБ/с	2500–5000	1500–3500	1000–3000

Це, у свою чергу, обумовлює необхідність розроблення нових засобів захисту інформації від витоку каналами ПЕМВН із значним розширенням частотного діапазону. Однак, нормативними документами, які визначають порядок проведення дослідження небезпечних сигналів, визначено діапазон частот, на яких проводиться вимірювання. Він складає 10 Гц – 1 ГГц.

Для досягнення поставленої у роботі мети запропоновано методику, яка складається з таких кроків: аналіз вихідних даних, зокрема протоколу СД, припису на експлуатацію об'єкта ЕОТ (ОТЗ) та схеми КЗ; підбір засобів захисту інформації (активного зашумлення), а також оцінювання ефективності впроваджених заходів (рівня захищеності інформації).

Узагальнену схему методики наведено на рис. 1. Варто зазначити, що кожен крок запропонованої методики – один із важливих елементів забезпечення необхідного рівня захищеності інформації, він не повинен розглядатися окремо або як заміна для будь-якого іншого.

Розглянемо кожен з них.

© Humeniuk I., Zaviriukha D., Kosterev D., Lahodnyi O., Sheihas V. Methodology for optimizing the selection of information protecting means from leakage by Transient Electromagnetic Pulse Emanation Standard // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 23-29. © This is an open access article under the CC BY 4.0 International license.*

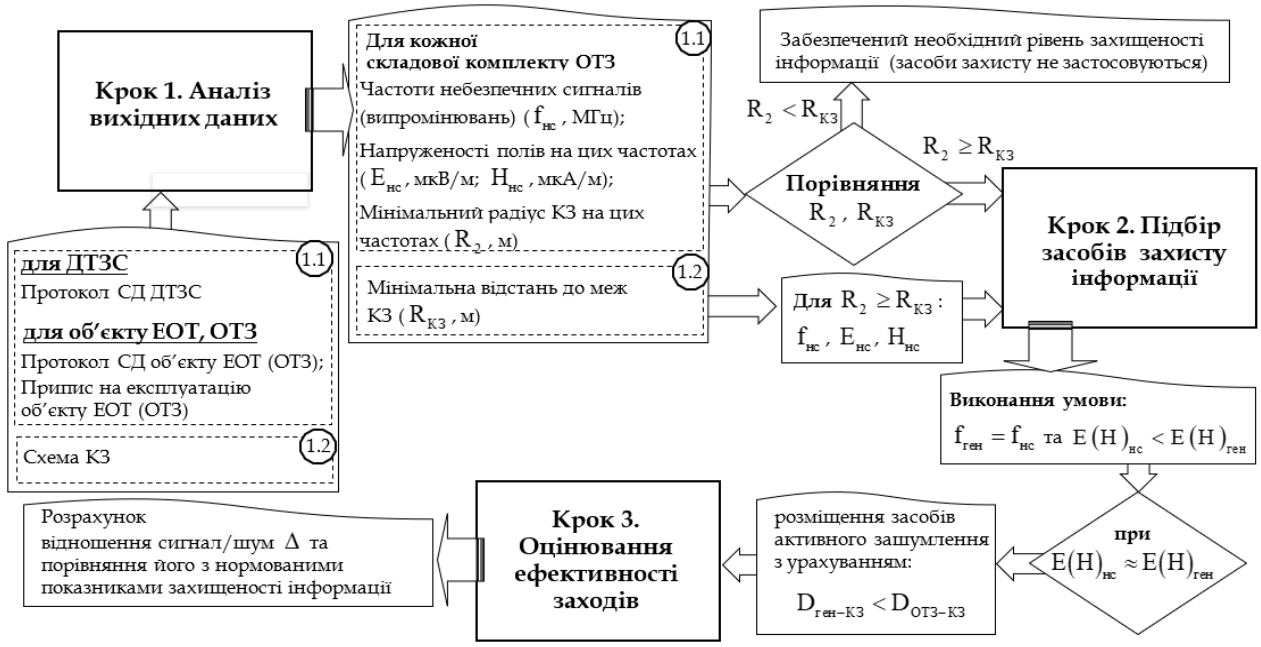


Рис. 1. Структурна схема методики оптимізації вибору засобів захисту інформації від витоку каналами ПЕМВН

На першому кроці проводиться аналіз вихідних даних, отриманих під час проведення СД ОІД або ОТЗ. При цьому для кожної складової ОТЗ визначаються частоти небезпечних сигналів (випромінювання) $f_{нс}$, які зазначаються у протоколі, а також значення напруженостей електричного $E_{нс}$ та магнітного полів $H_{нс}$, мінімального радіусу КЗ $R_{КЗ}$ на цих частотах. На підставі проведеного аналізу здійснюється порівняння радіусу зони 2 та мінімальної відстані до меж КЗ.

Зоною 2 є територія (сфера) навколо ОТЗ, за межами якої вважається неможливим перехоплення небезпечного сигналу з метою відтворення інформації. Така зона характеризується радіусом R_2, що визначає найбільшу відстань від технічних засобів оброблення інформації до межі, за якою напруженості електричного та магнітного полів небезпечного сигналу відносно шумових завад не перевищують нормованого значення. У цій зоні можливе перехоплення інформації, а за її межами – ні. Виходячи із цього твердження, умовою забезпечення необхідного рівня захищеності інформації від витоку технічними каналами ПЕМВН є $R_2 < R_{КЗ}$.

У протилежному випадку виконується крок вибору засобів захисту. Для його реалізації необхідними параметрами є значення частот небезпечних сигналів (випромінювання) та відповідних напруженостей електричного та магнітного полів. Вони обираються лише для тих величин мінімальної відстані до меж КЗ, які не перевищують розмір радіусу зони 2.

Підбір відповідних засобів активного зашумлення проводиться з урахування умов:

$$f_{ген} = f_{нс};\ E_{нс} < E_{ген};\ H_{нс} < H_{ген} \quad \text{при } R_2 \geq R_{КЗ}, \qquad (1)$$

де $f_{ген}$ – частоти маскувального сигналу (випромінювання) генератором радіочастотного шуму; $E_{ген}$, $H_{ген}$ – напруженості електричної та магнітної компонент електромагнітного поля генератором радіочастотного шуму відповідно на відстані 1 м.

За умови, що значення напруженостей полів небезпечного сигналу та генератора шуму майже однакові, місце розміщення засобу активного зашумлення обирається таким чином, щоб відстань між ним та межею КЗ $D_{ген-КЗ}$ була меншою ніж між ОТЗ та цією межею $D_{ОТЗ-КЗ}$.

Відповідно до [8] в Україні дозволені до використання засоби радіочастотного шуму "PIAC-1C", "PIAC-1M", засіб активного захисту інформації в автоматизованих систем "DELTA-7", фільтри електричні мережні "PIAC-4ФМ", ФЕМ-3 та ФЕМ-25, захисні протизавадні ФЗП 125-1, ФЗП 103-2 та ФЗП-110-2 тощо. Варто зазначити, що це не повний перелік сертифікованих засобів електромагнітного зашумлення. Характеристику таких засобів подано у табл. 1.

На останньому кроці проводиться оцінювання ефективності впроваджених заходів, зокрема здійснюється розрахунок відношення сигнал/шум Δ та порівняння його з нормованими показниками захищеності інформації.

Кінцевим результатом методики є обґрунтований вибір засобів активного електромагнітного зашумлення та їх розміщення, що забезпечує необхідний рівень захищеності інформації, яка обробляється на об'єкті ЕОТ.

© Humeniuk I., Zaviriukha D., Kosterev D., Lahodnyi O., Sheihas V. Methodology for optimizing the selection of information protecting means from leakage by Transient Electromagnetic Pulse Emanation Standard // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 23-29. © This is an open access article under the CC BY 4.0 International license.*

Таблиця 4

Засоби просторового електромагнітного зашумлення

Назва	Діапазон частот	Спектральна щільність напруженості		Максимальна значення вихідної потужності, Вт
		для діапазону частот	значення, дБ	
DELTA-7	9 кГц – 3,3 ГГц	15 кГц – 50 МГц	не менше 50	не менше 10
		50 МГц – 300 МГц	не менше 60	
		300 МГц – 500 МГц	не менше 50	
		500 МГц – 1,2 ГГц	не менше 40	
		1,2 ГГц – 2 ГГц	не менше 20	
PIAC- 1M	10 кГц – 1,5 ГГц	10 кГц – 500 МГц	не менше 50	не менше 5
		500 М Гц – 1 ГГц	не менше 40	
		1 ГГц – 1,5 ГГц	не менше 30	
PIAC-1C	180 Гц – 2 ГГц		30	не менше 10
PIAC-1C мод. 2	180 Гц – 2 ГГц		менше 30	не менше 10

Експериментальна частина

Верифікацію запропонованої методики проведено для об'єкту ЕОТ, на якому розміщений ОТЗ (табл. 5). Оброблення інформації з обмеженим доступом технічним засобом не здійснюється.

Таблиця 5

Характеристика складових ОТЗ

Назва складової	Модель
системний блок	
Материнська плата	MSI H201M_PRO-VDH_PLUS
ОЗП 8 ГБ	Transcend DDR4 2666
DWD-RW	Hitachi-LG SuperMulti GH24NSD5
SSD 2,5	GIGABYTE 4806B SATA TLC
периферійні пристрої	
Монітор	SAMSUNG S24D300H
Клавіатура	Genius Smart KM-200 Black
Принтер	Canon LBP-6030
Джерело безперебійного живлення	FSP DPV 650VA
Flash USB1	MUSIC
Flash USB2	ESD-USB

На першому кроці проведено аналіз вихідних даних, зокрема:

- зі схеми КЗ визначено мінімальну відстань до її межі, яка становить $R_{КЗ} = 32$ м;

- за результатами проведених СД оцінено значення частот небезпечних сигналів (випромінювань) складових ОТЗ, величини напруженостей електричного та магнітного полів та мінімальний радіус КЗ на цих частотах (табл. 6).

Порівнюючи R_2 та $R_{КЗ}$ встановлено що для таких складових:

- DWD-RW Hitachi-LG SuperMulti GH24NSD5;
- SSD 2,5 GIGABYTE 4806B SATA TLC;
- монітор SAMSUNG S24D300H;
- Flash USB1 MUSIC;
- Flash USB2 ESD-USB

забезпечений необхідний рівень захищеності інформації та, відповідно засоби захисту не застосовуються.

Таблиця 6

Результати вимірювань та розрахунків

№ з/п	$f_{нс}$, МГц	Напруженість поля		Радіус R_2, м
		$f_{нс}$, мкВ/м	$H_{нс}$, мкА/м	
Материнська плата MSI H201M_PRO-VDH_PLUS Не досліджується				
ОЗП 8 ГБ Transcend DDR4 2666 Не досліджується				
DWD-RW Hitachi-LG SuperMulti GH24NSD5				
Небезпечні сигнали не виявлені				
SSD 2,5 GIGABYTE 4806B SATA TLC				
1	2,5683	90,7	69,6	5
2	23,56853	47,7	11,9	5
3	213,7294	39,5	-	5
4	384,9483	31,6	-	5
5	991,9824	67,8	-	5
Монітор SAMSUNG S24D300H				
1	2,6162	48,1	-	5
2	74,2724	52,5	-	5
3	101,7265	45,3	-	5
4	373,2392	38,1	-	5
Клавіатура Genius Smart KM-200 Black				
1	2,6640	50,8	333,8	50
2	6,3007	81,0	122,3	40
3	19,1728	5,8	1,9	5
4	37,6425	13,3	4,6	5
5	38,1757	10,5	3,4	5
Принтер Canon LBP-6030				
1	91,1250	150,6	-	30
2	101,2958	340,2	-	70
3	382,6523	37,6	-	5
4	951,8369	61,9	-	5
5	954,2021	51,1	-	5
Flash USB1 MUSIC				
1	242,7460	33,1	-	5
2	599,9853	42,2	-	5
3	989,3027	68,1	-	5
Flash USB2 ESD-USB				
1	376,7324	110,5	-	20
2	599,9853	54,3	-	5
3	970,6347	65,2	-	5
4	989,3027	35,8	-	5
5	991,9824	98,4	-	15

У той же час для складових ОТЗ на небезпечних частотах (табл. 7) виконання умови $R_2 \geq R_{КЗ}$ обумовлює проведення підбору засобів захисту інформації.

© Humeniuk I., Zaviriukha D., Kosterev D., Lahodnyi O., Sheihas V. Methodology for optimizing the selection of information protecting means from leakage by Transient Electromagnetic Pulse Emanation Standard // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 23-29. © This is an open access article under the CC BY 4.0 International license.*

Таблиця 7

Результати виявлення небезпечних частот

№ з/п	$f_{нс}$, МГц	Напруженість поля		Радіус R_2, м
		$E_{нс}$, мкВ/м	$H_{нс}$, мкА/м	
Клавіатура Genius Smart KM-200 Black				
1	2,6640	50,8	333,8	50
2	6,3007	81,0	122,3	40
Принтер Canon LBP-6030				
1	91,1250	150,6	-	30
2	101,2958	340,2	-	70

Вибір засобів активного електромагнітного зашумлення (генераторів радіочастотного шуму) проводиться із урахуванням:

- випромінення електричної складової на частотах 91,1250 МГц та 101,2958 МГц з рівнем спектральної щільності напруженості поля на них більшою ніж 150,6 мкВ/м та 340,2 мкВ/м ;
- випромінення магнітної складової на частотах 2,6640 МГц та 6,3007 МГц з рівнем спектральної щільності напруженості поля на них більшою ніж 333,8 мкА/м та 122,3 мкА/м.

На останньому кроці методики здійснюється розрахунок відношення сигнал/шум та порівняння його з нормованими показниками захищеності інформації згідно чинних нормативних документів в галузі технічного захисту інформації.

Результати та їх обговорення

Аналіз отриманих результатів свідчить про те, що оптимізація вибору засобів захисту інформації від витоку ПЕМВН здійснюється з урахуванням рівнів небезпечних сигналів (випромінювань), відповідних зон їх поширення, енергетичних та спектральних показників, а також характеристик існуючих засобів активного електромагнітного зашумлення. Для досягнення необхідного рівня захищеності інформації варто виконувати комплексно усі кроки методики, а не розглядати їх окремо.

Висновки та перспективи подальших досліджень

У статті наведено результати вирішення актуального науково-практичного завдання, яке полягало в розробленні методики оптимізації вибору засобів захисту інформації від витоку каналами ПЕМВН на об'єкті ЕОТ. В її основу покладено: аналіз вихідних даних (частот небезпечних сигналів та інших параметрів на цих частотах), підбір засобів захисту інформації (активного зашумлення), а також оцінювання рівня захищеності інформації за рахунок впроваджених заходів.

Практичне цінність одержаних наукових результатів полягає в можливості використання запропонованої методики для забезпечення необхідного рівня захищеності інформації на об'єктах ЕОТ шляхом ефективного та оптимального вибору засобів електромагнітного зашумлення.

Виходячи із аналізу сучасних засобів оброблення інформації, перспективами подальшим досліджень є значне розширення частотного діапазону засобів активного електромагнітного зашумлення.

Список літератури

[1]. Гоков О. М. Фізичні основи технічних засобів розвідки: навчальний посібник. Харків : ХНЕУ ім. С. Кузнеця, 2022. 255 с.

[2]. Spectral Characteristics of Intermodulation Emissions during High-Frequency Imposition / L. Kriuchkova, I. Tsmokanych, N. Mazur, I. Chernihivskyi // CPITS 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems. 2025 (3991). pp. 449-462.

[3]. Скакун О. В., Воскресенський В. Б., Сивобородько А. В. Огляд портативних аналізаторів спектру та аналізаторів сигналів, що можуть бути використані під час виявлення побічних електромагнітних випромінювань // Вчені записки ТНУ ім. В. І. Вернадського. Серія: Технічні науки. 2021. Том 32 (71), № 3. С. 63–71.

[4]. Electromagnetic shielding as a method of protecting data processing equipment from information leaks / V. Kozlovsky, Y. Balanyuk, B. Zalevskyi, D. Kozlovska // Ukrainian Scientific Journal of Information Security. 2025. Vol. 31, Issue 2. pp. 74–79.

[5]. A TEMPEST Attack Implementation based on Hidden Markov model in Smart Grid / H. Qiao, K. Wang, T. Huang, X. Xu, S. Liu, J. Chen // Journal of Physics: Conference Series. 2024. 2774 (1). pp. 1–5.

[6]. Хлапонін Ю. І. Методика оцінки захищеності інформації від витоку каналом побічних електромагнітних випромінювань та наведень // Наукоємні технології. 2015. № 4 (28). С. 327–331.

[7]. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ : Вид-во НА СБ України, 2020. 256 с.

Перелік засобів ТЗІ, які мають експертний висновок про відповідність до вимог технічного захисту інформації. URL: cip.gov.ua/services/cm/api/attachment/download?id=64637

УДК 004.056.53:519.863

Humeniuk I.V., Zaviriukha D.O., Kosterev D.S., Lahodnyi O.V., Sheihas V.V. Methodology for optimizing the selection of information protecting means from leakage by Transient Electromagnetic Pulse Emanation Standard

Abstract. *The work substantiates and solves an important scientific and practical task, which consists in the development of a unique methodology for ensuring the protection of information from leakage through technical channels formed during its processing by appropriate means. The need for such a task is due to the high level of implementation of information threats through these channels, as well as the lack of universal methodical support for the implementation of measures to achieve the required level of information security. Normative documents in the field of technical information protection clearly outline the procedures of analytical and measuring works regarding the determination of information security indicators and the assessment of their compliance with the relevant norms. The proposed technique includes the following steps: analysis of initial data (frequencies of dangerous signals and other parameters at these frequencies), selection of information protection means (active noise), as well as assessment of the level of information security due to implemented measures. In addition, based on the analysis of modern means of information processing given in the work, prospects for further research on the need to significantly expand the frequency range of means of active*

electromagnetic noise are determined. The proposed technique is an important tool for building technical protection complexes at electronic computing facilities.
Key words: *Electronic-computing equipment objects, technical information leakage channel, Transient Electromagnetic Pulse Emanation Standard, information protection, dangerous signals, optimization.*

Гуменюк Ігор Володимирович, кандидат технічних наук, доцент, професор кафедри охорони державної таємниці та захисту інформації Житомирського військового інституту імені С.П Корольова
Humeniuk Ihor Volodymyrovych, candidate of technical sciences, Associate Professor, Professor at the Department of State Secrets Protection and Information Protection of Korolov Zhytomyr military institute

Завірюха Дмитро Олександрович, старший викладач кафедри охорони державної таємниці та захисту інформації Житомирського військового інститут ім. С.П. Корольова.
Zaviriukha Dmytro Oleksandrovych, Senior lecturer at the Department of State Secrets Protection and Information Protection of Korolov Zhytomyr Military Institute

Костерев Дмитро Сергійович, старший науковий співробітник науково-дослідного відділу розвитку інформаційної та кібернетичної безпеки науково-дослідного управління розвитку спеціальних систем та інновацій Житомирського військового інституту імені С. П. Корольова
Kosterev Dmytro Serhiyovych, Senior Researcher at the Research Department for Information and Cybersecurity Development, Research Directorate for Special Systems Development and Innovation of the Korolyov Zhytomyr Military Institute

Лагодний Олександр Васильович, кандидат технічних наук, доцент, заступник начальника кафедри охорони державної таємниці та захисту інформації Житомирського військового інституту імені С. П. Корольова
Lahodnyi Oleksandr Vasylovych, candidate of technical sciences, Associate Professor, Deputy Head at the Department of State Secrets Protection and Information Protection of the Korolov Zhytomyr military institute

Шейгас Віктор Вікторович, викладач кафедри охорони державної таємниці та захисту інформації Житомирського військового інституту ім. С.П. Корольова
Sheihas Viktor Viktorovych, lecturer at the Department of State Secrets Protection and Information Protection of Korolov Zhytomyr Military Institute

Дата надходження:	Дата прийняття:	Дата публікації:
19.06.2026	22.07.2026	21.08.2026