DOI: 10.18372/2310-5461.68.20237
УДК 621.391.82:004.056

***В. В. Козловский*,** д-р техн. наук, проф.
Державний університет «Київський авіаційний інститут», Київ
orcid.org/0000-0002-8301-5501
e-mail: vvkzeos@gmail.com;

Ю. В. Баланюк, д-р техн. наук, доцент,
Державний університет «Київський авіаційний інститут», Київ
orcid.org/0000-0003-3036-5804
e-mail: yurii.balaniuk@npp.kai.edu.ua;

Д. В. Козловська,
Державний університет "Київський авіаційний інститут, Київ
orcid.org/0009-0004-6223-0319
e-mail: vvkzeos@gmail.com;

Н. С. Вишневська
Державний університет "Київський авіаційний інститут", Київ
orcid.org/0000-0002-1358-467X
e-mail:nataliia.vyshnevska@npp.kai.edu.ua

ОБГРУНТУВАННЯ ПАРАМЕТРІВ ЕКРАНУЮЧИХ КОНСТРУКЦІЙ ДЛЯ ПРОТИДІЇ TEMPEST-ЗАГРОЗАМ

Вступ

В умовах цифрової трансформації забезпечення інформаційної безпеки переходить із площини прикладних інженерних рішень у ранг критичної умови, необхідної для стійкого функціонування та розвитку усіх ключових соціально-економічних і політичних систем. Захист інформації, що обробляється електронними засобами, є пріоритетом національної безпеки. TEMPEST-атаки є особливо небезпечними, оскільки вони дозволяють здійснювати несанкціоноване перехоплення даних (зокрема, з екранів, клавіатур, процесорів) на відстані, не залишаючи жодних слідів втручання у мережевій інфраструктурі. Ці випромінювання, що мимоволі генеруються електронними засобами обчислювальної техніки, можуть бути перехоплені та дешифровані зловмисниками, що робить пасивне фізичне спостереження надзвичайно ефективним каналом розвідки.

На сьогодні захист інформації розглядається як багаторівнева система, де фізичні методи є першим і найбільш фундаментальним рівнем оборони. Фізична безпека (як частина технічного захисту інформації) є необхідною умовою для ефективності усіх інших методів. Без на-дійного фізичного бар'єра (екрановані приміщення, захищені корпуси, контроль периметра) жоден криптографічний алгоритм чи програмний комплекс не може гарантувати конфіденційність інформації.

Таким чином, у сучасному високотехнологічному та насиченому електромагнітними полями середовищі, актуальність захисту інформації фізичними методами є критичним напрямком наукових досліджень та практично-го впровадження.

Постановка проблеми

В умовах зростаючої інтенсивності технічної розвідки та кібершпигунства, витік конфіденційної інформації через ненавмисні електромагнітні випромінювання, відомий як TEMPEST-загроза, залишається одним із найбільш прихованих і небезпечних каналів. Сучасне високопродуктивне електронне обладнання (сервери, комунікаційні системи) генерує потужні та широкосмугові ненавмисні електромагнітні випромінювання у діапазонах, що постійно розширюються. Це вимагає застосування спеціалізованих екрануючих конструкцій, які повинні гарантовано знижувати рівень випромінювання нижче порогу перехоплення.

Загалом, атаки на інформацію користувача поділяються на пасивні та активні [1]. Активна атака – це порушення кібербезпеки, під час якої неавторизований зловмисник безпосередньо втручається в цільову систему або мережу. Метою є зміна, видалення даних або порушення нормальної роботи системи. Зловмисники часто маскуються, щоб отримати доступ до конфіденційної інформації та використовувати або змінювати вже скомпрометовані дані для доступу до більш цінної інформації. Найпоширеніші типи активних

атак включають порушення нормального функціонування систем зв'язку, перехоплення та повторне надсилання повідомлення для імітації авторизації. Основним методом захисту від активних атак є впровадження таких заходів, як використання одноразових паролів, унікальних ключів сеансу для кожної транзакції, протоколів автентифікації.

Пасивна атака не впливає на передавач, приймач або дані, що передаються, а здійснюється з метою контролю або використання системних даних без будь-яких помітних змін або впливу на ресурси. Ці атаки важко виявити, і жертва часто не підозрює про їхнє існування. Основна мета – збір конфіденційної інформації або виявлення вразливих точок. Прикладом пасивної атаки є перехоплення та використання даних, що передаються між пристроями у мережі, часто із застосуванням спеціального програмного забезпечення для аналізу мережевого трафіку. Захист від пасивних атак досягається переважно через контроль доступу та шифрування даних. Використовуються два основні методи: шифрування із симетричним ключем (один спільний ключ для шифрування/дешифрування) та шифрування з відкритим ключем (публічний і закритий ключі для кожної сторони).

Атаки по бічному каналу та TEMPEST-загрози – це різновид пасивної атаки, що базується на непомітному моніторингу зв'язку шляхом використання фізичних факторів системи, таких як електромагнітне випромінювання, час обробки та споживання енергії. Основна мета такої атаки – використання ненавмисного електромагнітного випромінювання [2]. Ця проблема тісно пов'язана з компрометуючим електромагнітним випромінюванням [3], яке виникає навіть у пристроях, захищених криптографічними методами. Такі атаки часто включають фізичні вторгнення [4], коли зловмисник викрадає дані, спостерігаючи за фізичною поведінкою системи. Найкращою стратегією протидії є розробка систем шифрування, стійких до фізичного спостереження, шляхом впровадження методів балансування, засліплення та маскування. Для ефективного захисту також необхідний моніторинг незвичної поведінки в системі шифрування за допомогою датчиків, що фіксують споживання енергії або ЕМ-випромінювання. Перехоплення випромінюваних відеосигналів залишається серйозною проблемою електромагнітної безпеки [5].

Проблема полягає у відсутності уніфікованої, детально обґрунтованої інженерної методології, яка б забезпечувала надійний розрахунок і проєктування цих конструкцій відповідно до найсуворіших стандартів (наприклад, NATO SDIP-27). Існуючі підходи часто є надто спрощеними, зосереджуючись лише на загальній ефективності матеріалу, але ігноруючи або недостатньо деталізуючи необхідну точність розрахунків. Зокрема вибору таких фізичних параметрів екрана як товщина та матеріал, що є критичними для досягнення необхідного коефіцієнта екранування (≥ 100 дБ) у всьому критичному діапазоні частот. Проблематичним є питання мінімізації витоку ненавмисних електромагнітних випромінювань через технологічні отвори. Також на сьогодні відсутня обґрунтована процедура перевірки, яка гарантує, що розраховані та реалізовані параметри конструкції дійсно забезпечують необхідний рівень протидії TEMPEST-загрозам протягом усього терміну експлуатації.

Аналіз останніх досліджень і публікацій

На сьогодні значна кількість досліджень присвячена вивченню ненавмисного електромагнітного випромінювання як потенційного каналу витоку інформації [6–9].

Основними джерелами ненавмисного електромагнітного випромінювання є комп'ютерні периферійні пристрої. Окрему увагу приділено бездротовим клавіатурам, мишам та USB-адаптерам у дослідженні [6], в якому детально проаналізовано ризики перехоплення сигналів, незалежно від протоколів, шуму чи перешкод, а також розроблені профілактичні заходи проти зловмисної діяльності. Принтери, особливо ті, що використовуються в локальних мережах для великих обсягів друку, також є джерелами ненавмисного електромагнітного випромінювання [7–8]. Ці принтери зазвичай оснащені різними компонентами, такими як жорсткі диски, лінії живлення та сигналу, роз'єми та бездротові приймачі. Вимірювання електромагнітного випромінювання поблизу принтера дозволяє відновити надруковані дані.

Проблеми безпеки також спричиняє витік випромінювання через структурні провідники – сигнальні та силові лінії, телефонні кабелі та може спричинити численні проблеми безпеки [9]. Основний ризик тут полягає в тому, що ці провідники на високих частотах діють як антени, поширюючи компрометуючі сигнали за межі захищеної зони.

У сфері бездротових технологій особлива увага приділяється системам датчиків та RFID. Обробка та зберігання великих обсягів даних із датчиків, схильних до електромагнітних перешкод та індуктивного зв'язку, є предметом аналізу [10]. Зокрема, RFID-мітки через свою доступність є високовразливими до атак по бічних каналах, що підтверджується різними дослідженнями безпеки RFID [11].

датчиків, схильних до електромагнітних перешкод та індуктивного зв'язку, є предметом аналізу [10]. Зокрема, RFID-мітки через свою доступність є високовразливими до атак по бічних каналах, що підтверджується різними дослідженнями безпеки RFID [11].

Мета дослідження є обґрунтування та розробка рекомендацій щодо оптимізації ключових параметрів екрануючих конструкцій, здатних забезпечити не-обхідний рівень ослаблення побічних електромагнітних випромінювань в умовах сучасної високочастотної та динамічної електромагнітної обстановки.

Виклад основного матеріалу

Наразі електронне обладнання з мікропроцесорним керуванням, яке є важливим у телекомунікаційному та оборонному секторах, зазвичай працює у високочастотному діапазоні. Випромінювання на цих частотах є основним джерелом побічних електромагнітних випромінювань та наведень, які формують технічний канал витоку інформації. Особливість перехоплення інформації на високих частотах полягає у тому, що електромагнітне поле поширюється як плоска хвиля, несучи модульований конфіденційною інформацією сигнал. Методи дистанційного зчитування використовують спеціалізовану приймальну апаратуру, чутливу до високочастотного діапазону, для відновлення оброблюваних даних (криптографічних ключів, візуальної інформації тощо).

Застосування електромагнітного екрана при цьому може бути фізичним бар'єром, який не лише послаблює випромінювання, але й спотворює його характеристики. Спотворення є бажаним ефектом, оскільки воно критично ускладнює процес демодуляції та відновлення вихідних даних.

Вимоги TEMPEST (часто замінюється на EMSEC – Emissions Security) у військово-промисловій сфері є одними з найсуворіших у світі [12–13]. Вони стосуються захисту технічних засобів обробки даних від витоків інформації через побічні електромагнітні випромінювання та наведення. Це фактично стандарти на електромагнітне екранування та проєктування обладнання, які мають гарантувати, що важлива інформація (державна таємниця, військова інформація, криптографічні ключі) не може бути перехоплена зловмисником дистанційно шляхом аналізу цих випромінювань. Вимоги TEMPEST поділяються на кілька рівнів залежно від середовища, в якому використовується обладнання, та необхідної дистанції захисту. В НАТО для цього використовується стандарт SDIP-27 (раніше AMSG 720B/788A/784), який встановлює три основні рівні. Порівняльна характеристика рівнів TEMPEST-захисту за стандартами SDIP-27 (стандарт НАТО) та NSTISSAM (стандарт США) наведена у таблиці 1. Обладнання, що використовується для обробки секретної інформації у військово-промисловій сфері, повинно пройти обов'язкову сертифікацію TEMPEST в акредитованій лабораторії.

Таблиця 1

Порівняльна характеристика рівнів TEMPEST-захисту

Рівень TEMPEST	Стандарт SDIP-27	Стандарт NSTISSAM	Необхідна зона захисту	Основна вимога до захисту
A (FULL)	Level A	Level I	Зона 0 (найсуворіша)	Захист від безпосереднього перехоплення (наприклад, з сусідньої кімнати або на відстані близько 1 метра). Вимагає найвищого ступеня екранування.
B (IMMEDIATE)	Level B	Level II	Зона 1	Захист від перехоплення на відстані приблизно 20 метрів (як на відкритому просторі, так і крізь стіни).
C (TACTICAL)	Level C	Level III	Зона 2	Захист від перехоплення на відстані приблизно 100 метрів (призначений для тактичного та мобільного обладнання).

Обґрунтування параметрів екрануючих конструкцій для протидії TEMPEST-загроз базується на частотних характеристиках випромінювань, необхідному рівні їх ослаблення та конструктивних вимогах щодо цілісності екрана. Тобто, головною метою екранування проти TEMPEST-загроз є зниження рівня побічних електромагнітних випромінювань та наведень електронного обладнання до допустимого рівня, який унеможливлює відновлення конфіденційної інформації на відстані.

Плоскі екрани є фундаментальним елементом екрануючих конструкцій, що використовуються для протидії TEMPEST-загрозам. Їхнє основне завдання – забезпечити високе ослаблення побічних електромагнітних випромінювань від технічних засобів обробки даних через механізми відбиття та поглинання. Проходження електромагнітної хвилі через екран призводить до її спотворення та ослаблення, що є головною метою. Спотворення відбувається через те, що матеріал екрана взаємодіє з різними складовими та частотами хвилі порізному.

Матеріал для плаского екрана, що використовується для протидії TEMPEST-загрозам, має забезпечувати високу провідність для максимального відбиття та мати відповідні магнітні властивості для поглинання в широкому частотному діапазоні.

Для кількісного врахування дифракційних явищ застосовується коефіцієнт ефективності плаского екрана η екрана:

$$\eta = h_0 \cdot \cos\phi = \sqrt{\frac{2}{\lambda} \cdot \left(\frac{1}{R_1} + \frac{1}{R_2} \right)},$$

де η – коефіцієнт ефективності; φ – кут між векторами напрямів на кінці радіотіні; h_0 – відстань між кромкою екрана і віссю джерела; λ – довжина хвилі; R_1 – відстань від джерела до екрана; R_2 – відстань від екрана до зони захисту.

У реальності цей параметр дещо інший (рис. 1). Як показано на рис. 1, цей тип екранів демонструє надто високий коефіцієнт екранування (що не завжди є необхідною вимогою), їхнє практичне застосування часто обмежене.

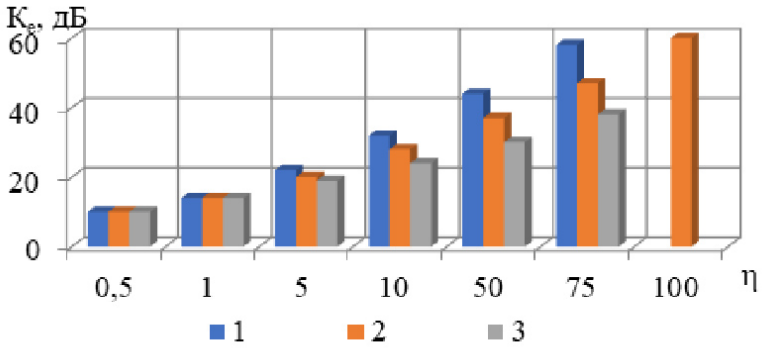

Рис. 1. Залежність коефіцієнта екранування від геометричних співвідношень розташування джерела поля та розмірів екрана: 1– для паралельного екрана складової поля, 2 – інтегральне екранування, 3 – для складової поля, перпендикулярної екрану

Перфоровані екрани є компромісом у TEMPEST-захисті, оскільки вони дозволяють забезпечити вентиляцію, охолодження або проходження світла, зберігаючи при цьому високий рівень ефективності екранування. Для протидії TEMPEST-загрозам критично важливо, щоб перфорація не перетворювалася на антену, яка випромінює побічні електромагнітні випромінювання.

Конструкції перфорованих екранів повинні задовольняти умови, що забезпечують необхідний мінімум захисту. Ефективності таких екранів залежать, в основному від діаметрів отворів d і відстаней між ними ℓ. Експериментальні дані щодо залежності коефіцієнта екранування перфорованих поверхонь і довжини електромагнітної хвилі λ та параметрів перфорації наведено на рис. 2.

Для ґратчастих і лінійних періодичних структур (чередування металевих дротів з визначеним кроком) коефіцієнти екранування залежать від діаметрів дротів та відстанями між їх осями, а також від довжини екранованої хвилі.

Залежності захисних властивостей таких екранів від згаданих параметрів наведено на рис. 3.

Для розрахунку ефективності екранування необхідно визначити напруженість електромагнітної хвилі, що здатна пройти крізь захисний матеріал. Відомо, що частки коефіцієнта екранування, які відповідають за відбиття та поглинання електромагнітної хвилі матеріалом, критично залежать від співвідношення хвильових опорів простору розповсюдження хвилі Z_0 та хвильового опору матеріалу екрана Z.

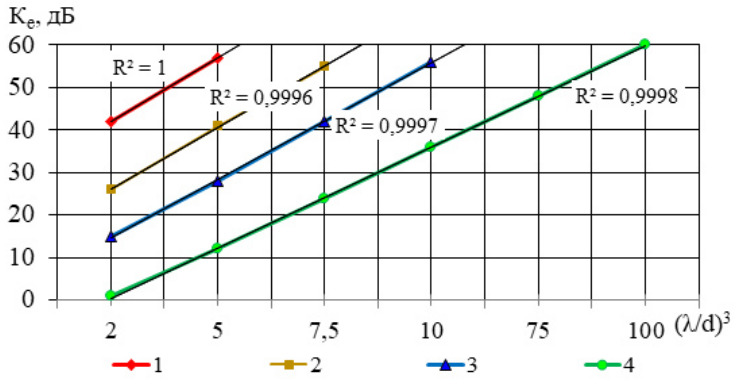

Рис. 2. Залежність захисних властивостей електромагнітного екрана від параметрів перфорації отворів ℓ: 1 – 50 мм, 2 – 20 мм, 3 – 10 мм, 4 – 5 мм

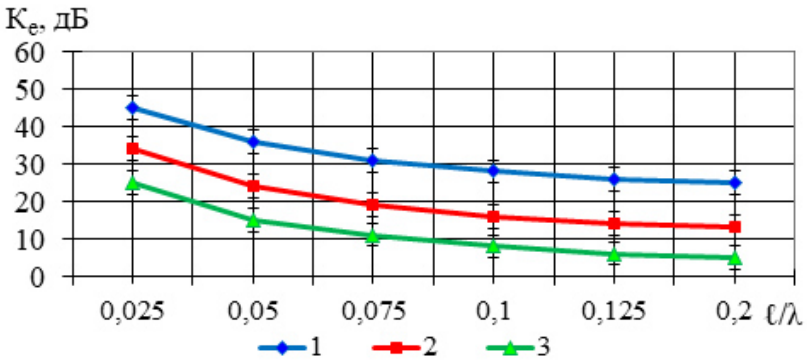

Рис. 3. Залежність коефіцієнта екранування електромагнітного поля від параметрів ґратчастої структури:
ℓ – відстань між осями дротів, d – діаметр дротів, λ – довжина хвилі;
1, 2, 3 – відповідають співвідношенням ℓ/d=2; 5; 10

При цьому:

$$Z_0 = \sqrt{\frac{\mu_0}{\varepsilon_0}}, \text{ а } Z = \sqrt{\frac{j\omega\mu}{\sigma + j\omega\varepsilon}},$$

де σ – провідність матеріалу екрана; μ – абсолютна магнітна проникність; ε – діелектрична проникність матеріалу; ω – циклічна частота поля.

Здійснивши стандартні перетворення, можна отримати значення коефіцієнтів екранування за рахунок відбиття та поглинання:

$$K_{\text{відб.}} = 20\lg\left(\frac{Z_0}{4Z}\right), \text{ дБ},$$

тобто, меншому опору матеріалу відповідають більші коефіцієнти відбиття. Щоб знизити коефіцієнт відбиття, потрібно наблизити значення хвильових опорів. Зазвичай опір вільного простору складає 377 Ом.

Отже, коефіцієнти відбиття залежать виключно від електрофізичних характеристик матеріалу екрана і не залежать від геометричних (товщини). Щодо коефіцієнтів поглинання, то цей показник є критичним.

При виборі товщини екрана необхідно враховувати еквівалентну глибину проникнення хвилі в екрануючий матеріал. Цей параметр визначається як відстань, від поверхні, на якій інтенсивність електромагнітного поля знижується в е разів (приблизно в 2,7 рази), що відповідає ослабленню на 8,7 децибела (дБ).

Розрахувати товщину екрана можна за співвідношенням:

$$\delta = \sqrt{\frac{2}{\omega\mu\sigma}}.$$

А коефіцієнт поглинання визначається як:

$$K_{\text{погл.}} = 20\lg e^{\Delta/\delta}, \text{ дБ},$$

де Δ – товщина екрана.

Слід зазначити, що хвильовий опір матеріалу екрана теж враховується при визначенні глибини проникнення завдяки його електрофізичним властивостям. Хоча для повної точності слід було б враховувати втрати від багаторазового відбиття електромагнітної хвилі у товщі екрана, на практиці цим внеском досить часто нехтують. Це пояснюється тим, що створення товстих екранів є неефективним. Натомість, оптимізація полягає у виборі матеріалу з високими електрофізичними характеристиками при збереженні мінімальної товщини конструкції.

Винятком є резонансні екрани. Вони розроблені таким чином, що тонкий шар провідного матеріалу, який поглинає енергію, розміщується точно на відстані, що дорівнює чверті довжини падаючої електромагнітної хвилі (λ/4), від провідної підкладки. Така конструкція забезпечує дуже високі поглинальні властивості, проте її ефективність обмежується дуже вузькою смугою частот.

Найбільш ефективні матеріали для екранування високочастотного та надвисокочастотного електромагнітного випромінювання (критичного для протидії загрозам безпеки інформації та методам захисту від цих загрози, це ті, що поєднують високу провідність (для відбиття) та здатність до поглинання електромагнітної енергії.

Для створення екранованих приміщень застосовують високопровідні матеріали, такі як мідь та алюміній. Їхня ефективність, особливо у високочастотному діапазоні, забезпечується домінуючим механізмом відбиття падаючої електромагнітної хвилі. Найвищу провідність серед економічно доступних металів, забезпечуючи винятковe ослаблення за рахунок відбиття має мідь.

Часто використовується у вигляді тонких листів або фольги в екранованих камерах. Дуже поширений через свою низьку вагу та ціну алюміній, має високу провідність, забезпечуючи відмінне ослаблення. Широко застосовується у будівництві екранованих приміщень та корпусів.

Для створення легких, тонких та широкосмугових екранів, а також для мінімізації перевипромінювання (реверберації) всередині приміщення,

використовують матеріали, які ефективно поглинають енергію. Це сучасні металополімерні матеріали.

Екрани такого типу характеризуються складним поєднанням відбивальних та поглинальних властивостей. Для визначення їхніх необхідних параметрів (за умови фіксованої концентрації металевих включень у діелектричні й матриці), можна застосувати розрахунок вхідного опору Z:

$$Z = \frac{Z_1 - jZ_2 tg(k_1 d)}{Z_2 - jZ_1 tg(k_2 d)} Z_2,$$

де Z_1 – хвильовий опір металу; Z_2 – хвильовий опір полімеру; k – хвильові числа; d – товщина екрана.

Перспективним напрямком для вдосконалення розрахункових моделей ефективності екранування є врахування не лише вагового вмісту металевих включень у діелектричній матриці, а й особливостей їхнього просторового розподілу у тілі екрана. Такий підхід дозволить поєднати переваги металополімерних та градієнтних екранів за рахунок підвищення ефективності захисту від електромагнітних полів, зокрема на ультрависоких і вищих частотах. Але для оцінювання захисних властивостей таких матеріалів необхідно мати експериментальні дані щодо магнітних та електрофізичних характеристик.

Розрахункові методи визначення рівнів та ефективності електромагнітних полів відіграють ключову роль у спрощенні процедури планування робіт з електромагнітної безпеки. Ці методи використовуються з метою прогнозування електромагнітної обстановки на стадії проєктування та при оптимізації розміщення електричного та електронного обладнання у виробничому середовищі. Важливо, що за рахунок застосування розрахункових методів можливо врахувати фактичні електрофізичні властивості матеріалів і компонентів конструкцій. Це дає змогу попередньо оцінити захисні властивості матеріалів і, відповідно, значно зменшити обсяг дорогих тестових випробувань у процесі проектування захисту від електромагнітних полів.

Висновки

Проведене дослідження доводить, що в умовах цифрової трансформації та зростання кіберзагроз фізичний захист інформації від ненавмисних електромагнітних випромінювань, набуває статусу критичної умови національної безпеки. TEMPEST-атаки, як різновид пасивних атак, є особливо небезпечними, оскільки дозволяють непомітно перехоплювати дані залишаючись непомітними.

Обґрунтовано, що для ефективної протидії сучасним TEMPEST-загрозам, особливо у високочастотному діапазоні, екрануючі конструкції повинні забезпечувати гарантований коефіцієнт загасання, що відповідає найсуворішим стандартам (зокрема, Level A/I за SDIP-27/NSTISSAM) та вимагає SE ≥ 100 дБ.

Встановлено, що ключові параметри екрана, а саме коефіцієнти відбиття та поглинання, критично залежать від співвідношення хвильових опорів простору та матеріалу екрана, а також від глибини проникнення хвилі у тіло екрана. Це підтверджує, що ефективність захисту досягається не лише товщиною, а й оптимізацією електрофізичних характеристик матеріалу.

Визначено, що найбільш перспективними для широкосмугового екранування лектронного обладнання є металополімерні матеріали, що мають високу провідність для відбиття та здатність до поглинання електромагнітної енергії.

Впровадження розрахункових методів для прогнозування захисних властивостей матеріалів є перспективним для мінімізації обсягу натурних випробувань та спрощення процедури планування робіт з електромагнітної безпеки на етапі проєктування.

ЛІТЕРАТУРА

[1] Pawar M. V., Anuradha J. Network security and types of attacks in network. *Procedia Computer Science.* 2015. Vol. 48. PP. 503–506. https://doi.org/10.1016/j.procs.2015.04.126

[2] Grdović M. M., Protić D. D., Antić V. D., Jovanović B. Ž. Screen reading: Electromagnetic information leakage from the computer monitor. *Vojnotehnicki glasnik Military Technical Courier. 2022*. Vol. 70(4). PP. 836–855. DOI: https://doi.org/10.5937/vojtehg70-38930

[3] Markagic, Milorad. Compromising electromagnetic radiation: Challenges, threats and protection. *Vojnotehnicki glasnik*. 2018. Vol. 66. PP. 143–153. DOI:https://doi.org/10.5937/vojtehg66-8691.

[4] Barthe G., Grégoire B., Laporte V. Secure compilation of side-channel countermeasures: the case of cryptographic «constant-time». In *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*.2018. PP. 328–343. IEEE. DOI: 10.1109/CSF.2018.00031

[5] Uribe, J. D. J. R., Guillen, E. P., & Cardoso, L. S. (2022). A technical review of wireless security for the internet of things: Software defined radio perspective. *Journal of King Saud University-Computer and Information Sciences*, *34*(7), 4122–4134. DOI: https://doi.org/10.1016/j.jksuci.2021.04.003

[6] Jovanovic S. V., Protic D. D., Antic V. D., Grdovic M. M., Bajic D. A. Security of wireless keyboards: Threats, vulnerabilities and countermeasures. *Vojnoteh. Mil.*

Tech. Cour. 2023, *71*, PP. 296–315. DOI: https://doi.org/10.5937/vojtehg71-43239
[7] Kubiak I., Loughry J. LED Arrays of Laser Printers as Valuable Sources of Electromagnetic Waves for Acquisition of Graphic Data. *Electronics*. 2019. *8*(10), 1078. DOI:https://doi.org/10.3390/electronics8101078
[8] Burmester, M.; de Medeiros, B. RFID Security: Attacks, Countermeasures and Challenges. URL: https://www.cs.fsu.edu/~burmeste/133.pdf
[9] Huzurbazar S., Kuang D., Lee L. Landmark-based algorithms for group average and pattern recognition. *Pattern Recognition*. 2019. Vol. 86. PP. 172–187. DOI: https://doi.org/-10.1016/j.patcog.2018.09.002
[10] Toledo J. I., Carbonell M., Fornes A., Llados J. Information extraction from historical handwritten document images with a context-aware neural model. *Pattern Recognition*. 2019, Vol. 86. PP. 27–36.
[11] Semertzis, A. Ștefanov, A. Presekal, B. Kruimer, J. L. R. Torres and P. Palensky, «Power System Stability Analysis From Cyber Attacks Perspective» in IEEE Access, VOL. 12. PP. 113008–113035, 2024. DOI: 10.1109/ACCESS.2024.3443061.
[12] NSA. TEMPEST: A Signal Problem. Approved for Release by NSA on 09-07-2007, FOIA Case #51633, 26–30. URL: https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-spectrum/tempest.pdf
[13] AC/322-D/(2019)0041-REV 1, Technical and Implementation Directive on Introducing Secure Systems and Solutions Using Commercial-off-the-Shelf Products (COTS) in NATO, 20 April 2021.

Козловський В. В., Баланюк Ю. В., Козловська Д. В., Вишневська Н. С.

ОБГРУНТУВАННЯ ПАРАМЕТРІВ ЕКРАНУЮЧИХ КОНСТРУКЦІЙ ДЛЯ ПРОТИДІЇ TEMPEST-ЗАГРОЗАМ

В епоху цифрової трансформації та ескалації загроз кібершпигунства, фізичний захист інформації набуває статусу критичної умови для забезпечення національної безпеки. Стаття присвячена дослідженню та обґрунтуванню інженерних параметрів екрануючих конструкцій, спрямованих на ефективну протидію TEMPEST-загрозам. Актуальність дослідження посилюється зростаючою інтенсивністю та широкосмуговістю випромінювань, які генерує сучасне високопродуктивне обладнання (сервери, комунікаційні системи), що вимагає застосування спеціалізованих захисних рішень. Обґрунтовано рекомендацій щодо оптимізації ключових фізичних параметрів екрануючих конструкцій, необхідних для забезпечення гарантованого рівня ослаблення побічних електромагнітних випромінювань відповідно до міжнародних стандартів. Надано порівняльну характеристику рівнів TEMPEST-захисту за стандартами SDIP-27 та NSTISSAM. Доведено, що ефективність екрана досягається завдяки двом основним механізмам – відбиття (домінує на високих частотах) та поглинання електромагнітної хвилі матеріалом. Розрахункові формули коефіцієнтів відбиття та поглинання демонструють їхню критичну залежність від співвідношення хвильових опорів і товщини екрана. Розглянуто особливості плоских та перфорованих екранів. Успішна протидія TEMPEST-загрозам полягає у синергії між матеріалом та конструкцією. Встановлено, що найбільш перспективними для широкосмугового захисту є матеріали, які поєднують високу провідність та здатність до поглинання. Доведено, що впровадження розрахункових методів на етапі проєктування дозволяє прогнозувати захисні властивості матеріалів, враховуючи просторовий розподіл металевих включень, що значно мінімізує обсяг дороговартісних натурних випробувань та спрощує процедуру планування робіт з електромагнітної безпеки. Результати дослідження є фундаментальною основою для розробки інженерних рішень, що відповідають найвищим вимогам міжнародної електромагнітної безпеки.

Ключові слова: інформаційна безпека, TEMPEST-загроза, пасивна атака, електромагнітне екранування, екрануючі конструкції, фізичний захист інформації.

Kozlovsky V., Balanyuk Y, Kozlovska D., Vyshnevska N.

JUSTIFICATION OF THE PARAMETERS OF SHIELDING STRUCTURES TO COUNTER TEMPEST THREATS

In the era of digital transformation and escalation of cyber espionage threats, physical protection of information acquires the status of a critical condition for ensuring national security. The article is devoted to the study and justifica-tion of engineering parameters of shielding structures aimed at effective counteraction to TEMPEST threats. The rele-vance of the study is enhanced by the growing intensity and broadband of radiation generated by modern high-perfor-mance equipment (servers, communication systems), which requires the use of specialized protective solutions. Recom-mendations are substantiated for optimizing key physical parameters of shielding structures necessary to ensure a guar-anteed level of attenuation of side electromagnetic radiation in accordance with international standards. A comparative characteristic of TEMPEST protection levels according to SDIP-27 and NSTISSAM standards is provided. It is proven that the effectiveness of the screen is achieved due to two main mechanisms - reflection (dominant at high frequencies)

and absorption of electromagnetic waves by the material. The calculated formulas for the reflection and absorption coefficients demonstrate their critical dependence on the ratio of wave resistances and screen thickness. The features of flat and perforated screens are considered. Successful counteraction to TEMPEST threats lies in the synergy between the material and the design. It has been established that the most promising for broadband protection are materials that combine high conductivity and absorption capacity. It has been proven that the implementation of calculation methods at the design stage allows predicting the protective properties of materials, taking into account the spatial distribution of metal inclusions, which significantly minimizes the volume of costly full-scale tests and simplifies the procedure for planning electromagnetic safety work. The results of the study are a fundamental basis for developing engineering solutions that meet the highest requirements of international electromagnetic safety.

Keywords: information security, TEMPEST threat, passive attack, electromagnetic shielding, shielding structures, physical protection of information.

Стаття надійшла до редакції 29.10.2025 р.
Прийнято до друку 10.12.2025 р.