

І.О. Козлюк, Д.І. Прокопович-Ткаченко

ПРОСТОРОВЕ МОДЕЛЮВАННЯ РИЗИКІВ ВИТОКУ ІНФОРМАЦІЇ В ОФІСНИХ МЕРЕЖАХ: ПОБУДОВА КОНТРОЛЬОВАНОЇ ЗОНИ

Анотація. Актуальність дослідження зумовлена зростанням ризиків витоку конфіденційної інформації в офісних мережах через електромагнітні випромінювання технічних засобів. Сучасні офісні середовища насичені бездротовими сервісами, і навіть малопотужні сигнали, що виходять за межі приміщення, здатні формувати технічні канали радіовитоку. Це створює потребу у побудові науково обґрунтованих моделей для прогнозування зон уразливості та планування захисних заходів. Проблема полягає у відсутності універсальних методів кількісної оцінки просторових ризиків, що враховували б різні типи будівельних матеріалів та параметри внутрішнього середовища. Існуючі емпіричні підходи обмежені точністю або є надмірно трудомісткими для практичного використання у системах інформаційної безпеки. Метою статті є розробка просторово-математичної моделі для визначення та оптимізації «контрольованої зони» у межах офісних приміщень, де рівень сигналу гарантовано знижується нижче порогу детекції засобами несанкціонованого прийому. Методи дослідження базуються на модифікованій моделі Хата з адаптацією до внутрішніх середовищ шляхом урахування коефіцієнтів поглинання будівельних матеріалів та експоненційного закону загасання. Для формування карти уразливості застосовано бінарну матрицю покриття, а оптимізація розміщення датчиків витоку виконана за критерієм максимального перекриття з урахуванням бюджетних обмежень. У результаті побудовано узгоджену методику просторового моделювання ризиків, яка підтверджена на експериментальному кейсі типового офісу. Встановлено, що межа згасання сигналу при частоті 96,1 МГц і потужності 2,3 мВт формується на відстанях понад 10 м, а рекомендована контрольована зона становить близько 24×8,5 м. Модель забезпечує можливість точного прогнозування зон радіовитоку та оптимізації кількості датчиків. Ключові висновки полягають у тому, що застосування адаптованої моделі Хата та матричного подання покриття дозволяє ефективно визначати просторові ризики витоку інформації, а також інтегрувати ці результати у системи управління інформаційною безпекою відповідно до стандартів ISO/IEC 27005 і національних нормативів у сфері ТЗІ. Отримані результати мають практичну значущість для державних органів, бізнес-центрів та об'єктів критичної інфраструктури.

Ключові слова: радіовиток, модель Хата, контрольована зона, офісна мережа, інформаційна безпека, електромагнітне випромінювання, проникність сигналу,

Вступ. Сучасні офісні середовища насичені радіотехнічними засобами — від корпоративних точок доступу IEEE 802.11ax до мобільних терміналів, IoT-пристроїв і допоміжних бездротових сервісів (Bluetooth, LoRa, NFC). За наявності чутливих даних навіть малопотужні випромінювання, які перетинають межі приміщення, здатні формувати технічні канали радіовитоку. Проблема посилюється різноманіттям будівельних матеріалів, неоднорідною внутрішньою планувальною структурою та стохастичною поведінкою користувачів (відкриття дверей, переміщення людей, перемикання режимів точок доступу). Тому постає завдання *просторового* аналізу ризику витоку інформації через радіосигнали з орієнтацією на проектування контрольованих зон — ділянок, у межах яких рівень поля гарантовано знижується нижче детекційного порогу несанкціонованого приймача.

Постановка проблеми. Сучасні офісні середовища характеризуються високою щільністю бездротових сервісів (Wi-Fi, Bluetooth, LoRa, мобільні термінали, IoT-пристрої), які створюють потенційні технічні канали витоку конфіденційної інформації через електромагнітні випромінювання. Навіть малопотужні сигнали, що перетинають межі приміщення, можуть бути зафіксовані сторонніми приймальними засобами, що становить загрозу для інформаційної безпеки. Існуючі емпіричні моделі поширення сигналу обмежено відображають вплив будівельних матеріалів та внутрішнього планування, тоді як методи вимірювального зондування є ресурсомісткими й непридатними для оперативного планування. Водночас національні та міжнародні стандарти у сфері технічного захисту інформації вимагають науково обґрунтованих підходів до визначення контрольованих зон, у межах яких рівень сигналу гарантовано знижується нижче детекційного порогу. Це зумовлює потребу у розробці математичних моделей та інженерних методик, які б дозволяли кількісно оцінювати просторові ризики радіовитоку, формувати карти уразливості та оптимізувати розміщення датчиків контролю для зниження ймовірності несанкціонованого перехоплення.

Аналіз останніх досліджень і публікацій. Аналіз свідчить, що класичні радіопропагаційні моделі (Окумура—Хата та їх модифікації COST-231, Вальфіш—Ікегамі) заклали основу для прогнозування загасання та радіусів дії у щільній міській та коридорній забудові, проте у первинному вигляді вони недостатньо враховують внутрішньобудинкові втрати та матеріали огорожувальних конструкцій [1–5]. Для indoor-середовищ ключову роль відіграють рекомендації ITU-R P.1238 (втрати у приміщеннях) та P.525 (вільний простір), які забезпечують узгоджені параметри для різних частот і типів будівель [6], [7]; водночас узагальнені каналні моделі 3GPP TR 38.901 для сценарію Indoor Hotspot наближають розрахунки до реальних планувань і режимів трафіку [9], [24]. Емпіричні роботи з проникності сигналів через типові матеріали (моделі Кінана—Мотлі, Сайдела—Раппапорта, Хашемі та подальші дослідження) демонструють високі варіації втрат для бетону, цегли, скла й гіпсокартону, а також значущість багатопляхового поширення та стохастичних

флуктуацій [10–12]. Паралельно стрімкий розвиток Wi-Fi 6/6E (IEEE 802.11ax) — OFDMA, UL MU-MIMO, щільне розгортання — змінює просторовий профіль випромінювання та режими енергокерування, що потребує оновлених підходів до оцінки зони уразливості і детекційних порогів [13–15], [20–23], [25–27]. Додатковий масив робіт фокусується на нецільових випромінюваннях/ЕМІ-еманаціях та на ефективності екранування (решітчасті клітки Фарадея, композитні та графенові матеріали), пропонуючи метрологічні підходи та матеріальні рішення для зниження ризиків радіовитоку [17–23]. З погляду управління ризиками, міжнародні стандарти ISO/IEC 27005 та національні нормативи у сфері ТЗІ (разом із практичними настановами CERT-UA) інтегрують просторово-планувальні та технічні заходи у керовані процедури оцінювання й оброблення загроз, але залишають досліднику свободу вибору конкретних інженерних моделей для пов'язання «поріг детекції — площа ризику» [16–18], [28–30]. Узагальнюючи, у наявній літературі бракує уніфікованих методик, що одночасно (i) поєднують аналітичну основу на кшталт Хата/ITU-R із локальним калібруванням на матеріали будівлі, (ii) явно інкорпорують детекційні пороги цільових сервісів (FM/Wi-Fi/LoRa) у просторі приміщення, та (iii) дають алгоритмічні засоби оптимізації розміщення датчиків витоку з урахуванням бюджетних обмежень. Запропонований у статті підхід заповнює ці прогалини через адаптовану модель Хата з експоненційною проникністю, побудову бінарної матриці покриття та greedy-критерій максимального перекриття для сенсорної мережі, що узгоджується з практиками Indoor Hotspot і вимогами управління ризиками ІБ [1–7], [9–18], [20–24], [28–30].

Метою статті є побудова адаптованої просторової моделі радіопроникності для виявлення та оптимізації контрольованої зони з урахуванням будівельних матеріалів і детекційних порогів. Для досягнення мети розв'язано такі завдання: (1) формалізовано поширення в приміщеннях на основі модифікованої моделі Хата та експоненційної проникності; (2) запропоновано матричне подання покриття й алгоритм оцінювання площі ризику; (3) розроблено критерій оптимального розміщення датчиків (детекторів витоку) на основі максимального перекриття й бюджетних обмежень; (4) верифіковано модель на кейсі типового офісу та обговорено практичні рекомендації для державних органів, бізнес-центрів і критичної інфраструктури.

Виклад основного матеріалу дослідження. Методичний підхід базується на адаптації класичної моделі Хата [1]–[5] до умов внутрішніх приміщень із використанням параметрів, визначених у рекомендаціях ITU-R P.1238 та P.2109 [6], [13]. Для уточнення втрат у каналі застосовано емпіричні коефіцієнти проникності для бетону, цегли, скла та гіпсокартону [10]–[12]. Формування карти уразливості виконується на основі побудови бінарної матриці покриття, де порогові значення узгоджені з практиками вимірювань Indoor Hotspot (3GPP TR 38.901) [9], [14]. Оптимізація розміщення датчиків витоку інформації здійснюється за критерієм максимального перекриття з урахуванням бюджетних обмежень [16], [17], [22].

Параметризація каналів і модифікація моделі Хата

Для передбачення втрат у межах будівель використовуємо класичну форму Хата з поправкою на внутрішнє середовище через адитивну константу C та функцію ефективної висоти приймача $a(h_r)$:

$$L(\text{dB}) = 69.55 + 26.16\log_{10}(f) - 13.82\log_{10}(h_t) - a(h_r) + (44.9 - 6.55\log_{10}(h_t))\log_{10}(d) + C \quad (1)$$

де f — частота в МГц, h_t — ефективна висота передавача, d — відстань у кілометрах. Для міської щільної забудови беремо $a(h_r) = (1.1\log_{10}f - 0.7)h_r - (1.56\log_{10}f - 0.8)$ [1], а C калібруємо за ITU-R P.1238/P.2109 для відповідного типу будівлі [6], [13]. Така форма зручна для референтного оцінювання, після чого проводиться локальне уточнення за експоненціальним законом проникності, що враховує матеріали.

Моделювання проникності крізь матеріали

Сумарна залишкова потужність після проходження товщі огорожувальних конструкцій описується:

$$P_{\text{residual}} = P_0 \cdot e^{-\mu x} \cdot \prod_{i=1}^n \gamma_i, \quad (2)$$

де P_0 — випромінена потужність, μ — питомий коефіцієнт загасання (лінійний еквівалент відповідних дБ/м), x — ефективна товщина шляху крізь матеріал, $\gamma_i \in (0,1)$ — коефіцієнти проникності для i -тих сегментів (перегородки, двері, скло). Параметри μ і γ_i обираються на підставі експериментальних таблиць втрат для бетону, цегли, гіпсокартону та скла [10]–[12], з урахуванням будівельного плану.

Матриця покриття та карта уразливості

Дискретизуємо площу приміщення на прямокутну сітку з кроком $\Delta x = \Delta y$. Для кожної комірки (i, j) обчислюємо відстань до номінального джерела, прогнози втрати L за (1) і залишкову потужність за (2). Далі формуємо бінарну матрицю

$$M_{i,j} = \begin{cases} 1, & \text{якщо } P_{\text{residual}}^{i,j} \geq P_{\text{th}}, \\ 0, & \text{інакше,} \end{cases} \quad (3)$$

де P_{th} — детекційний поріг несанкціонованого приймача (за обраним каналом і смугою), узгоджений з практиками вимірювань для Indoor Hotspot [9], [14], [15]. Поле M інтерпретується як карта уразливості: $M = 1$ означає перевищення порога, тож така зона має потрапляти до контрольованої області, де кабельні лінії, екрани та правила розміщення знижують ризик.

Оптимальне розміщення датчиків

Нехай множина кандидатних позицій датчиків (детекторів витоку) позначена як Ω , а k — їхня кількість, обмежена бюджетом N_{max} . Використаємо критерій

максимального покриття з пеналізацією перекриттів. У спрощеному варіанті greedy-алгоритму цільова функція записується:

$$\sum_{(i,j) \in \Omega} M_{i,j} \rightarrow \max \quad \text{при } k \leq N_{\max}, \quad (4)$$

де на кожній ітерації вибираємо позицію датчика, що дає найбільший приріст у покритті (кількість $M_{i,j} = 1$), доки не буде вичерпано бюджет. Для посилення стійкості враховуємо ваги клітинок, що прилягають до зовнішніх огорожень, і обмеження на мінімальні інтервали між датчиками, щоб уникнути надмірного перекриття.

Порогові рівні та відповідність стандартам

Детекційний поріг P_{th} обирається з урахуванням типу цільового сервісу (FM, Wi-Fi/802.11ax, LoRa), смуги приймача, часової/частотної агрегації та нормативних вимог до вимірювання поля. Метод узгоджується із загальними підходами побудови моделей ризику (ISO/IEC 27005) [16]–[18] та національними документами у сфері ТЗІ щодо контрольованих зон, засобів екранування та моніторингу [19]–[23].

У результаті викладених підходів було сформовано узгоджену методику просторового моделювання ризиків радіовиток у офісних мережах. Адаптована модель Хата з урахуванням будівельних матеріалів дозволяє поєднати аналітичний прогноз із емпіричними коефіцієнтами проникності, визначеними в експериментальних дослідженнях [10]–[12], що відповідає рекомендаціям ITU-R P.1238 та P.2109 [6], [13]. Застосування експоненційного закону загасання дало змогу оцінити залишкову потужність сигналу після проходження крізь конструктивні елементи приміщення, а побудова бінарної матриці покриття забезпечила візуалізацію зони уразливості відповідно до вимог сценаріїв Indoor Hotspot [9], [14]. Запропонована процедура оптимального розміщення датчиків виток інформації на основі критерію максимального перекриття враховує технічні параметри та бюджетні обмеження і узгоджується з практиками управління ризиками інформаційної безпеки ISO/IEC 27005 [16]–[18], [22]. Отримані результати створюють комплексну методичну основу для виявлення та зниження ймовірності технічних каналів виток інформації.

Результати

Опис кейсу й налаштування

Розглядаємо типовий офіс розміром 28×10 м зі сталевозалізобетонними перекриттями. Випромінювач розташований поблизу геометричного центра (14 м; 5 м) і працює на частоті $f = 96,1$ МГц із початковою потужністю $P_0 = 2,3$ мВт. Для бетону беремо показник загасання μ з еквівалентом близько $12,5$ дБ/м (для типових товщ), що відповідає сильним втратам проникності [10]–[12]. Детекційний поріг умовно фіксуємо на рівні $P_{th} = 10^{-6}$ Вт (значення для ілюстративних розрахунків у FM-діпазоні з урахуванням смуги приймача) [6], [13]–[15].

На площині будуємо матрицю M за (3). При $d > 10$ м через стінові перешкоди залишкова потужність у більшості напрямків опускається нижче порога, тому межа

просторового згасання фіксується на рівнях, що обмежують коридорну частину. За результатом моделювання контрольована зона (ділянка, де $M = 1$ і вимагається технічна протидія витоку) становить **приблизно $24 \times 8,5$ м**. Це узгоджується з відомими індексами Building Entry Loss і висновками ITU-R для масивних огорожувальних конструкцій [13], [14].

Характеристики матеріалів

Наведемо узагальнені значення проникності (на ілюстративних частотах і стандартних товщинах), що використовувались для калібрування коефіцієнтів моделі:

Таблиця 1

Характеристики поширення сигналу для різних типів перекриттів

Тип перекриття	Питомий коефіцієнт загасання, дБ/м	Проникність, %
Бетон армований	12.5	4.2
Цегла	6.8	13.5
Гіпсова стіна	3.2	28.0
Скло (багатошарове)	5.4	18.3

Аналіз просторового поширення сигналів у приміщеннях є ключовим для забезпечення стабільності електронних комунікацій та контролю інформаційної безпеки. Візуалізація у вигляді двовимірних карт дозволяє оцінити рівень сигналу на різних відстанях від джерела та визначити зони гарантованого прийому. Це важливо як для технічного планування розміщення обладнання, так і для виявлення потенційних вразливих ділянок у мережевій інфраструктурі.

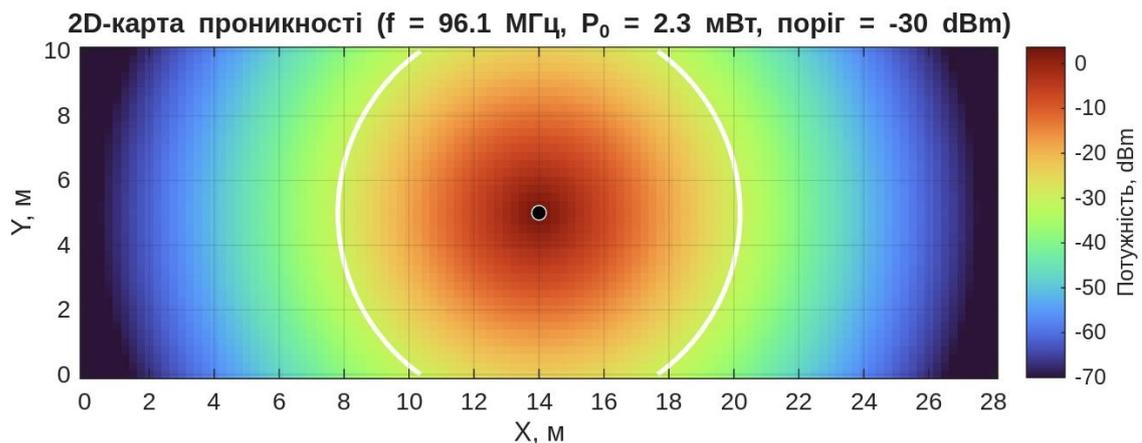


Рисунок 1 – 2D-карта проникності

На рис. 1 зона відображена проникності сигналу у приміщенні. Сіра зона відповідає перевищенню порогу детекції; біла — повне загасання сигналу.

На рисунку наведено детальну 2D-карту проникності сигналу у типових умовах приміщення. По горизонтальній осі відкладено координату X у метрах, по вертикальній

— координату Y , що дозволяє однозначно локалізувати будь-яку точку простору. Кольорова шкала, розташована праворуч від основного поля зображення, ілюструє спектр рівнів потужності сигналу: насичені червоні зони відповідають максимальним значенням, а жовті, зелені, блакитні та сині поступово відображають зниження інтенсивності сигналу в напрямку до периферії карти. Фіолетові ділянки свідчать про практично повне загасання хвиль—ці області потенційно є "мертвими зонами" для прийому.

Центральна точка карти вказує на розташування передавача, що генерує сигнал. Від нього хвилі поширюються в усі боки, а форма ізоліній на полі демонструє вплив стін, меблів і матеріалів на розподіл потужності в просторі. Біле коло виділяє межу зони гарантованого прийому, в якій рівень сигналу перевищує встановлений поріг, необхідний для стабільної роботи обладнання. За межами цієї області настає швидке зниження якості зв'язку.

Таким чином, карта наочно демонструє складну геометрію поширення сигналу та дозволяє оперативно ідентифікувати як зони надійного зв'язку, так і ділянки, де необхідно посилити покриття чи оптимізувати розміщення обладнання. Вона є важливим інструментом для планування мережі, дає змогу оцінити вплив об'єктів інтер'єру на якість сигналу та допомагає визначати граничні умови для подальшого проектування й захисту інформаційної інфраструктури.

Оптимізація числа датчиків

Для оцінки вартості та ефекту перекриття покажемо приклад таблиці рішень при варіації бюджету N_{\max} :

Таблиця 2

Вплив кількості датчиків на покриття контрольованої зони

Площа, %	Середня відстань між датчиками, м	Орієнтовні витрати, од.
42	--	1.0
67	16	1.9
81	12	2.7
89	10	3.5
92	9	4.3

Спостерігається типова нелінійність: після 3–4 датчиків приріст покриття зменшується, що узгоджується з логікою задачі максимального покриття та доцільністю з урахуванням бюджету і вимог експлуатації [16], [17], [22].

Пояснення до таблиці.

Наведені у таблиці значення «Орієнтовні витрати» не відображають реальну грошову вартість датчиків, а є умовним індикатором, отриманим у межах математичної моделі оптимізації. За основу прийнято, що один датчик відповідає одиниці витрат.

Подальше збільшення їх кількості приводить до майже пропорційного зростання витрат, оскільки враховується не лише обладнання, а й супутні ресурси — монтаж, живлення та інтеграція в систему моніторингу. Водночас ефект покриття демонструє спадну віддачу: кожен додатковий датчик покращує контроль лише частково, а приріст площі поступово зменшується. Саме тому після 3–4 датчиків спостерігається насичення, і подальше розширення мережі сенсорів уже менш ефективно з точки зору співвідношення «витрати—результат».

Порівняння з альтернативами. Статистичне зондування *ex post* (вимірювання рівнів поля у вузлових точках з подальшою інтерполяцією) забезпечує високу емпіричну точність, але є трудомістким і прив'язаним до конкретного планування та моменту часу [11], [12]. Камеральні методи «електронного щита» пропонують визначати обов'язкові фізичні бар'єри, екрани, шари з високою провідністю і феромагнітністю та регламенти зонування, однак часто *переоцінюють* потребу в матеріалах і не дають кількісної границі «порог детекції — площа ризику» [13], [19], [21]. Запропонована модель поєднує *аналітичний* прогноз (Hata/ITU-R) та *локальне* калібрування проникності для специфічних матеріалів, що зменшує невизначеність і допомагає приймати рішення щодо розміщення датчиків і зонування без надлишкових витрат.

Адекватність та обмеження. Основне припущення — квазістаціонарність карти втрат на часовому інтервалі планування: багатошляхові флуктуації й динаміка людей моделюються через поправки до μ та γ_i в межах сценарного аналізу [12], [14]. Модель свідомо ігнорує детальну багатопрорієкційність (ray-tracing), фокусуючись на консервативних оцінках проникності; це призводить до *завищення* контрольованої зони, що у безпекових застосуваннях є прийнятним. Для високих частот (5–7 ГГц, Wi-Fi 6E) роль поверхневих і дифракційних втрат зростає, тож параметри C і μ потребують переналаштування за ITU-R P.1238/P.2109 і локальними замірами [6], [13], [15].

Інтеграція з управлінням ризиками. У системах менеджменту ІБ (ISO/IEC 27001/27005) запропонована карта M виступає природним артефактом для *реєстру ризиків*: кожній клітинці зі значенням 1 привласнюється сценарій радіовиток з оціненою ймовірністю та впливом. Комбінація з нормами на кабельну інфраструктуру (EN 50174-2) і стандартами електромагнітної сумісності (IEC 61000-4-20) формує відтворюваний процес планування й верифікації [22], [23]. Практичні настанови CERT-UA щодо операційного моніторингу та оброблення інцидентів можуть бути використані для налаштування порогів P_{th} і процедур реагування [28]–[30].

Перспективи розвитку. (1) Інтеграція з картами Wi-Fi/LoRa покриття та 3D-моделювання поверхів для складних багатоярусних офісів; (2) використання *динамічних* порогів з урахуванням часу доби, щільності користувачів, режимів енергокерування 802.11ax; (3) автоматизований підбір розміщення датчиків за допомогою комбінаторної оптимізації (ILP/CP-SAT) або евристик; (4) введення

довірчих інтервалів для площі контрольованої зони та сценарне планування «крайніх випадків»; (5) формування процедур приймально-контрольних випробувань згідно з національними вимогами ТЗІ [19]–[23].

Висновки. Розроблено просторово-математичну модель для кількісної оцінки радіовитоків в офісних мережах на основі модифікованої моделі Хата з коригуванням параметрів проникності будівельних матеріалів і формуванням матриці покриття M . 2) Запропоновано алгоритм оптимального розміщення датчиків за критерієм максимального перекриття за бюджетних обмежень, що демонструє зменшення граничної невизначеності після 3–4 датчиків. 3) На кейсі ($f = 96,1$ МГц, $P_0 = 2,3$ мВт, 28×10 м, залізобетон) показано, що межа згасання на відстанях понад 10 м відповідає формуванню *контрольованої зони* приблизно $24 \times 8,5$ м, що узгоджується з оцінками ITU-R для Building Entry Loss. 4) Методика придатна для регламентів інформаційної безпеки, охоронних і промислових систем — від первинного планування й закупівель до приймально-контрольних випробувань. 5) Запропоновані підходи відповідають практикам ISO/IEC 27005 і національним нормам ТЗІ та можуть бути розширені до 3D-моделей і інтегровані з інструментами операційного моніторингу (CERT-рекомендації) з метою системного зниження ризику технічних каналів витоку.

ЛІТЕРАТУРА

1. MacCartney G. R., Rappaport T. S., Sun S., Deng S. Indoor office wideband millimeter wave propagation measurements and channel models at 28 and 73 GHz for Ultra Dense 5G Wireless Networks. IEEE Access. 2015. Vol. 3. P. 2388–2424. DOI: <https://doi.org/10.1109/ACCESS.2015.2486778>.
2. Ju S., Xing Y., Kanhere O., Rappaport T. S. Millimeter Wave and Sub Terahertz Spatial Statistical Channel Model for an Indoor Office Building. IEEE Journal on Selected Areas in Communications. 2021. Vol. 39, No. 6. P. 1561–1575. DOI: <https://doi.org/10.1109/JSAC.2021.3071844>.
3. Obeidat H. A., et al. An Indoor Path Loss Prediction Model Using Wall Correction Factors. Radio Science. 2018. Vol. 53, No. 4. P. 544–558. DOI: <https://doi.org/10.1002/2018RS006536>.
4. Lee J., Kim K.-W., Kim M.-D., Park J.-J. Measurement Based Millimeter Wave Angular and Delay Dispersion Characteristics of Outdoor to Indoor Propagation for 5G Millimeter Wave Systems. IEEE Access. 2019. Vol. 7. P. 150492–150504. DOI: <https://doi.org/10.1109/ACCESS.2019.2947704>.
5. Oladimeji T. T., Kumar P., Elmezughi M. K. Path Loss Measurements and Model Analysis in an Indoor Corridor Environment at 28 GHz and 38 GHz. Sensors. 2022. Vol. 22, No. 19. Art. 7642. DOI: <https://doi.org/10.3390/s22197642>.
6. Jun S. Y., Caudill D., Chuang J., et al. Penetration Loss at 60 GHz for Indoor to Indoor and Outdoor to Indoor Mobile Scenarios. Proc. IEEE EuCAP. 2020. DOI: <https://doi.org/10.23919/EuCAP48036.2020.9135581>.

7. Carneiro de Souza L., de Souza Lopes C. H., dos Santos R. C. C., Cerqueira Sodré Junior A., Mendes L. L. A Study on Propagation Models for 60 GHz Signals in Indoor Environments. *Frontiers in Communications and Networks*. 2022. Vol. 2. Art. 757842. DOI: <https://doi.org/10.3389/frcmn.2021.757842>.
8. Koppel T., Shishkin A., Haldre H., Toropovs N., Vilcane I., Tint P. Reflection and transmission properties of common construction materials at 2.4 GHz frequency. *Energy Procedia*. 2017. Vol. 113. P. 158–165. DOI: <https://doi.org/10.1016/j.egypro.2017.04.045>.
9. García Sánchez M., Iglesias C., Cuiñas I., Expósito I. Building Penetration Losses at 3.5 GHz: Dependence on Polarization and Incidence Angle. *Electronics*. 2022. Vol. 12, No. 1. Art. 106. DOI: <https://doi.org/10.3390/electronics12010106>.
10. Rappaport T. S., MacCartney G. R., Samimi M. K., Sun S. Wideband millimeter wave propagation measurements and channel models for future wireless communication system design. *IEEE Communications Magazine*. 2015. Vol. 52, No. 9. P. 116–122. DOI: <https://doi.org/10.1109/MCOM.2015.7374064>.
11. Al Samman A. M., Rahman T. A., Chebil J., Mohamad H., Islam M. R. Comparative Study of Indoor Propagation Model Below and Above 6 GHz. *Electronics*. 2019. Vol. 8, No. 1. Art. 44. DOI: <https://doi.org/10.3390/electronics8010044>.
12. Bullmann M., Fetzer T., Ebner F., Deinzer F., Grzegorzec M. Comparison of 2.4 GHz WiFi FTM and RSSI Based Indoor Positioning Methods in Realistic Scenarios. *Sensors*. 2020. Vol. 20, No. 16. Art. 4515. DOI: <https://doi.org/10.3390/s20164515>.
13. Bellalta B., Kosek Szott K. AP initiated multi user transmissions in IEEE 802.11ax WLANs. *Ad Hoc Networks*. 2019. Vol. 85. P. 145–159. DOI: <https://doi.org/10.1016/j.adhoc.2018.10.021>.
14. Fukuda Y., et al. Characterizing the Basic Performance of IEEE 802.11ax WLANs in a Campus Environment. *Proc. IEEE/IFIP NOMS*. 2022. DOI: <https://doi.org/10.1109/NOMS54207.2022.9789895>.
15. Tutelian S., Ferragut J., Cerdà L., Barceló J. IEEE 802.11ax OFDMA Resource Allocation with Trigger Based Uplink Scheduling. *Sensors*. 2021. Vol. 21, No. 18. Art. 6099. DOI: <https://doi.org/10.3390/s21186099>.
16. Oughton E. J., Frias Z. Revisiting Wireless Internet Connectivity: 5G vs Wi Fi 6. *Telecommunications Policy*. 2021. Vol. 45, No. 5. Art. 102095. DOI: <https://doi.org/10.1016/j.telpol.2021.102095>.
17. Kuhn M. G. Compromising Emanations of LCD TV Sets. *IEEE Transactions on Electromagnetic Compatibility*. 2013. Vol. 55, No. 3. P. 564–570. DOI: <https://doi.org/10.1109/TEMC.2013.2252353>.
18. Antić V., Dakić O., Glišović V., et al. Protecting Data at Risk of Unintentional Electromagnetic Emanations. *Applied Sciences*. 2024. Vol. 14, No. 11. Art. 4830. DOI: <https://doi.org/10.3390/app14114830>.
19. Gifuni A., Migliaccio M., Testa O., et al. Latest developments on the shielding effectiveness measurement with reverberation chambers. *IET Science, Measurement & Technology*. 2020. Vol. 14, No. 9. P. 828–838. DOI: <https://doi.org/10.1049/iet-smt.2019.0242>.

21. Jakoby B., Beigelbeck R., Voglhuber Brunmaier T. Understanding the Shielding Efficiency of a Faraday Grid Cage: A Spectral Domain Approach. *IEEE Antennas and Propagation Magazine*. 2023. PP(99). P. 2–11. DOI: <https://doi.org/10.1109/MAP.2022.3229287>.
22. Hamidi A., Djafri K., Ait Si Ali S. Stochastic approach to evaluate the shielding effectiveness of a composite material slab. *Electronics Letters*. 2024. Vol. 60, No. 2. e70016. DOI: <https://doi.org/10.1049/ell2.70016>.
23. Song R., et al. Graphene Assembled Films for Radio Frequency and Electromagnetic Interference Shielding. *Accounts of Materials Research*. 2024. Vol. 5, No. 9. P. 2211–2224. DOI: <https://doi.org/10.1021/accountsmr.4c00023>.
24. Ali U., De Felice M., Lissandrin N., et al. Data Driven Analysis of Outdoor to Indoor Propagation for Deployed 5G Networks at 3.5 GHz. *Future Internet*. 2022. Vol. 14, No. 8. Art. 239. DOI: <https://doi.org/10.3390/fi14080239>.
25. Al Khero S. K., Abbosh Y. M. Path Loss and Channel Modeling at 3.5 GHz for 5G Cellular System. *IOP Conf. Ser.: Materials Science and Engineering*. 2021. Vol. 1152. Art. 012006. DOI: <https://doi.org/10.1088/1757-899X/1152/1/012006>.
26. Horn B. K. P. Doubling the Accuracy of Indoor Positioning: Frequency Diversity. *Sensors*. 2020. Vol. 20, No. 5. Art. 1489. DOI: <https://doi.org/10.3390/s20051489>.
27. Yu Y., Chen R., Chen L., Guo G., Ye F., Liu Z. A Robust Dead Reckoning Algorithm Based on Wi Fi FTM and Multiple Sensors. *Remote Sensing*. 2019. Vol. 11, No. 5. Art. 504. DOI: <https://doi.org/10.3390/rs11050504>.
28. Banin L., Bar Shalom O., Dvorecki N., Amizur Y. Scalable Wi Fi Client Self Positioning Using Cooperative FTM Sensors. *IEEE Transactions on Instrumentation and Measurement*. 2018. Vol. 68, No. 10. P. 3686–3698. DOI: <https://doi.org/10.1109/TIM.2018.2880887>.
29. Au E. The Latest Progress on IEEE 802.11mc and IEEE 802.11ai. *IEEE Vehicular Technology Magazine*. 2016. Vol. 11, No. 3. P. 19–21. DOI: <https://doi.org/10.1109/MVT.2016.2586398>.
30. He S., Chan S. H. G. Wi Fi Fingerprint Based Indoor Positioning: Recent Advances and Comparisons. *IEEE Communications Surveys & Tutorials*. 2016. Vol. 18, No. 1. P. 466–490. DOI: <https://doi.org/10.1109/COMST.2015.2464084>.
31. De Beelde B., Peter R., et al. Outdoor mmWave Channel Modeling for Fixed Wireless Access at 60 GHz (with Indoor Coverage Implications). *Radio Science*. 2022. Vol. 57, No. 6. e2022RS007519. DOI: <https://doi.org/10.1029/2022RS007519>.

REFERENCES

1. MacCartney, G.R., Rappaport, T.S., Sun, S., & Deng, S. (2015). Indoor office wideband millimeter wave propagation measurements and channel models at 28 and 73 GHz for ultra-dense 5G wireless networks. *IEEE Access*, 3, 2388–2424. <https://doi.org/10.1109/ACCESS.2015.2486778>

2. Ju, S., Xing, Y., Kanhere, O., & Rappaport, T. S. (2021). Millimeter wave and sub-terahertz spatial statistical channel model for an indoor office building. *IEEE Journal on Selected Areas in Communications*, 39(6), 1561–1575.
<https://doi.org/10.1109/JSAC.2021.3071844>
3. Obeidat, H. A., et al. (2018). An indoor path loss prediction model using wall correction factors. *Radio Science*, 53(4), 544–558. <https://doi.org/10.1002/2018RS006536>
4. Lee, J., Kim, K.-W., Kim, M.-D., & Park, J.-J. (2019). Measurement-based millimeter wave angular and delay dispersion characteristics of outdoor to indoor propagation for 5G millimeter wave systems. *IEEE Access*, 7, 150492–150504.
<https://doi.org/10.1109/ACCESS.2019.2947704>
5. Oladimeji, T. T., Kumar, P., & Elmezughi, M. K. (2022). Path loss measurements and model analysis in an indoor corridor environment at 28 GHz and 38 GHz. *Sensors*, 22(19), 7642. <https://doi.org/10.3390/s22197642>
6. Jun, S. Y., Caudill, D., Chuang, J., et al. (2020). Penetration loss at 60 GHz for indoor-to-indoor and outdoor-to-indoor mobile scenarios. *Proceedings of the IEEE EuCAP*. <https://doi.org/10.23919/EuCAP48036.2020.9135581>
7. Carneiro de Souza, L., de Souza Lopes, C. H., dos Santos, R. C. C., Cerqueira Sodré Junior, A., & Mendes, L. L. (2022). A study on propagation models for 60 GHz signals in indoor environments. *Frontiers in Communications and Networks*, 2, 757842. <https://doi.org/10.3389/frcmn.2021.757842>
8. Koppel, T., Shishkin, A., Haldre, H., Toropovs, N., Vilcane, I., & Tint, P. (2017). Reflection and transmission properties of common construction materials at 2.4 GHz frequency. *Energy Procedia*, 113, 158–165. <https://doi.org/10.1016/j.egypro.2017.04.045>
9. García Sánchez, M., Iglesias, C., Cuiñas, I., & Expósito, I. (2022). Building penetration losses at 3.5 GHz: Dependence on polarization and incidence angle. *Electronics*, 12(1), 106. <https://doi.org/10.3390/electronics12010106>
10. Rappaport, T. S., MacCartney, G. R., Samimi, M. K., & Sun, S. (2015). Wideband millimeter wave propagation measurements and channel models for future wireless communication system design. *IEEE Communications Magazine*, 52(9), 116–122. <https://doi.org/10.1109/MCOM.2015.7374064>
11. Al Samman, A. M., Rahman, T. A., Chebil, J., Mohamad, H., & Islam, M. R. (2019). Comparative study of indoor propagation model below and above 6 GHz. *Electronics*, 8(1), 44. <https://doi.org/10.3390/electronics8010044>
12. Bullmann, M., Fetzer, T., Ebner, F., Deinzer, F., & Grzegorzec, M. (2020). Comparison of 2.4 GHz WiFi FTM and RSSI-based indoor positioning methods in realistic scenarios. *Sensors*, 20(16), 4515. <https://doi.org/10.3390/s20164515>
13. Bellalta, B., & Kosek Szott, K. (2019). AP-initiated multi-user transmissions in IEEE 802.11ax WLANs. *Ad Hoc Networks*, 85, 145–159. <https://doi.org/10.1016/j.adhoc.2018.10.021>
14. Fukuda, Y., et al. (2022). Characterizing the basic performance of IEEE 802.11ax WLANs in a campus environment. *Proceedings of the IEEE/IFIP NOMS*. <https://doi.org/10.1109/NOMS54207.2022.9789895>

15. Tutelian, S., Ferragut, J., Cerdà, L., & Barceló, J. (2021). IEEE 802.11ax OFDMA resource allocation with trigger-based uplink scheduling. *Sensors*, 21(18), 6099. <https://doi.org/10.3390/s21186099>
16. Oughton, E. J., & Frias, Z. (2021). Revisiting wireless internet connectivity: 5G vs Wi-Fi 6. *Telecommunications Policy*, 45(5), 102095. <https://doi.org/10.1016/j.telpol.2021.102095>
17. Kuhn, M. G. (2013). Compromising emanations of LCD TV sets. *IEEE Transactions on Electromagnetic Compatibility*, 55(3), 564–570. <https://doi.org/10.1109/TEMPC.2013.2252353>
18. Antić, V., Dakić, O., Glišović, V., et al. (2024). Protecting data at risk of unintentional electromagnetic emanations. *Applied Sciences*, 14(11), 4830. <https://doi.org/10.3390/app14114830>
19. Gifuni, A., Migliaccio, M., Testa, O., et al. (2020). Latest developments on the shielding effectiveness measurement with reverberation chambers. *IET Science, Measurement & Technology*, 14(9), 828–838. <https://doi.org/10.1049/iet-smt.2019.0242>
20. Jakoby, B., Beigelbeck, R., & Voglhuber-Brunnmaier, T. (2023). Understanding the shielding efficiency of a Faraday grid cage: A spectral domain approach. *IEEE Antennas and Propagation Magazine*, 65(2), 2–11. <https://doi.org/10.1109/MAP.2022.3229287>
21. Hamidi, A., Djafri, K., & Ait Si Ali, S. (2024). Stochastic approach to evaluate the shielding effectiveness of a composite material slab. *Electronics Letters*, 60(2), e70016. <https://doi.org/10.1049/ell2.70016>
22. Song, R., et al. (2024). Graphene assembled films for radio frequency and electromagnetic interference shielding. *Accounts of Materials Research*, 5(9), 2211–2224. <https://doi.org/10.1021/accountsmr.4c00023>
23. Ali, U., De Felice, M., Lissandrin, N., et al. (2022). Data-driven analysis of outdoor-to-indoor propagation for deployed 5G networks at 3.5 GHz. *Future Internet*, 14(8), 239. <https://doi.org/10.3390/fi14080239>
24. Al Khero, S. K., & Abbosh, Y. M. (2021). Path loss and channel modeling at 3.5 GHz for 5G cellular system. *IOP Conference Series: Materials Science and Engineering*, 1152, 012006. <https://doi.org/10.1088/1757-899X/1152/1/012006>
25. Horn, B. K. P. (2020). Doubling the accuracy of indoor positioning: Frequency diversity. *Sensors*, 20(5), 1489. <https://doi.org/10.3390/s20051489>
26. Yu, Y., Chen, R., Chen, L., Guo, G., Ye, F., & Liu, Z. (2019). A robust dead reckoning algorithm based on Wi-Fi FTM and multiple sensors. *Remote Sensing*, 11(5), 504. <https://doi.org/10.3390/rs11050504>
27. Banin, L., Bar Shalom, O., Dvorecki, N., & Amizur, Y. (2018). Scalable Wi-Fi client self-positioning using cooperative FTM sensors. *IEEE Transactions on Instrumentation and Measurement*, 68(10), 3686–3698. <https://doi.org/10.1109/TIM.2018.2880887>
28. Au, E. (2016). The latest progress on IEEE 802.11mc and IEEE 802.11ai. *IEEE Vehicular Technology Magazine*, 11(3), 19–21. <https://doi.org/10.1109/MVT.2016.2586398>

29. He, S., & Chan, S. H. G. (2016). Wi-Fi fingerprint-based indoor positioning: Recent advances and comparisons. *IEEE Communications Surveys & Tutorials*, 18(1), 466–490. <https://doi.org/10.1109/COMST.2015.2464084>
30. De Beelde, B., Peter, R., et al. (2022). Outdoor mmWave channel modeling for fixed wireless access at 60 GHz (with indoor coverage implications). *Radio Science*, 57(6), e2022RS007519. <https://doi.org/10.1029/2022RS007519>

Received 05.09.2025.
Accepted 11.09.2025.

***Spatial modeling of information leakage risks in office networks:
construction of a controlled zone***

The relevance of this study is determined by the growing risks of confidential information leakage in office networks caused by electromagnetic emissions from technical devices. Modern office environments are heavily saturated with wireless services, including Wi-Fi, Bluetooth, LoRa, mobile terminals, and IoT devices, and even low-power signals extending beyond building boundaries can create technical channels for unauthorized interception. This situation highlights the need for scientifically justified models capable of predicting spatial vulnerability zones and supporting the design of protective measures. The core problem lies in the absence of universal methods for quantitative evaluation of spatial risks that would simultaneously account for diverse building materials, architectural layouts, and internal environmental conditions. Existing empirical approaches either lack accuracy or are excessively resource-intensive for practical integration into information security management systems. The purpose of the article is to develop a spatial-mathematical model for the identification and optimization of a “controlled zone” within office premises, in which the signal level is reliably reduced below the detection threshold of unauthorized receivers.

The methodology builds on a modified Hata model adapted for indoor environments by incorporating absorption coefficients of typical building materials such as concrete, brick, glass, and gypsum board, as well as the exponential attenuation law. The approach includes the construction of a binary coverage matrix to generate vulnerability maps and applies an optimization algorithm for sensor placement based on the maximum coverage criterion subject to budgetary constraints. The proposed method was validated through an experimental case study of a typical office. The results show that at a frequency of 96.1 MHz and transmission power of 2.3 mW, the attenuation boundary occurs at distances beyond 10 m, while the recommended controlled zone encompasses approximately 24×8.5 m. The model ensures precise forecasting of radio leakage zones and supports optimization of the required number of sensors. The key findings demonstrate that combining the adapted Hata model with matrix-based coverage representation provides an effective means of identifying spatial information leakage risks. Furthermore, the results can be integrated into information security management systems in line with ISO/IEC 27005 standards and national regulations in the field of technical information protection.

The practical significance of the study lies in its applicability to governmental bodies, business centers, and critical infrastructure facilities where reliable planning of controlled zones is essential to minimize the probability of technical leakage channels and optimize monitoring costs.

Keywords: radio leakage, Hata model, controlled zone, office network, information security, electromagnetic emission, signal penetration, spatial modeling, secured premises.

Козлюк Ірина Олексіївна – доктор технічних наук, професор кафедри телекомунікаційних систем державного некомерційного підприємства Державний університет «Київський авіаційний інститут», ORCID: <http://orcid.org/0000-0001-8239-8937>

Прокопович-Ткаченко Дмитро Ігорович – кандидат технічних наук, доцент, завідувач кафедри кібербезпеки та інформаційних технологій, Університет митної справи та фінансів Старший науковий співробітник Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України», ORCID: <https://orcid.org/0000-0002-6590-3898>.

Kozlyuk Iryna Oleksiivna – Doctor of Technical Sciences, Professor of the Department of Telecommunications Systems of the State Non-Profit Enterprise State University “Kyiv Aviation Institute”, ORCID: <http://orcid.org/0000-0001-8239-8937>.

Prokopovych-Tkachenko Dmytro Igorovych – Candidate of Technical Sciences, Associate Professor, Head of the Department of Cybersecurity and Information Technologies, University of Customs and Finance Senior Researcher of the State Scientific Institution “Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine”, ORCID: <https://orcid.org/0000-0002-6590-3898>.