



DOI 10.28925/2663-4023.2025.28.812

УДК 004.056

Лаптев Олександр Анатолійович

д.т.н., с.н.с., доцент кафедри кібербезпеки та захисту інформації

КНУ імені Тараса Шевченка, Київ, Україна

ORCID ID: 0000-0002-4194-402X

olaptiev@knu.ua**Лаптева Тетяна Олександрівна**

PhD з кібербезпеки, Державний торговельно-економічний університет

ORCID ID: 0000-0002-5223-9078

tetiana1986@ukr.net**Браїловський Микола Миколайович**

к. т. н., доцент кафедри кібербезпеки та захисту інформації

КНУ імені Тараса Шевченка, Київ, Україна

ORCID ID: 0000-0002-3148-1148

bk1972@ukr.net**МЕТОДИКИ РОЗРАХУНКІВ ПАРАМЕТРІВ
ВИЯВЛЕННЯ СИГНАЛІВ ЗАСОБІВ НЕГЛАСНОГО ОТРИМАННЯ
ІНФОРМАЦІЇ (ДЖЕРЕЛ РАДІОВИПРОМІНЮВАННЯ)**

Анотація. У статті представлено методику оцінювання ключових параметрів виявлення сигналів засобів негласного отримання інформації, зокрема джерел радіовипромінювання. Запропоновано послідовний алгоритм розрахунків, який дозволяє прогнозувати середній час виявлення джерела радіовипромінювання, ймовірність його розкриття за допустимий час спостереження та ефективність виявлення надкоротких передач. Особлива увага приділена аналізу електромагнітної доступності, що є критичним фактором при виявленні слабких сигналів на фоні завад. Для цього розроблено детальну послідовність розрахунків, яка включає визначення потужності сигналу на вході приймача, врахування характеристик антен, поляризаційного та просторового узгодження, втрат в фідерах, додаткового ослаблення радіохвиль у залежності від умов поширення, а також порівняння реальної та необхідної потужності для забезпечення заданої ймовірності виявлення. Розглянуто задачу визначення ймовірності радіовипромінювання при виявленні короткочасних сигналів. Отримані формули враховують тривалість випромінювання, швидкість сканування діапазону частот, період перегляду діапазону та час, необхідний для первинного технічного аналізу сигналу. Це дозволяє прогнозувати ймовірність виявлення сигналів заданої тривалості в реальних умовах експлуатації. Методика може бути використана при проектуванні нових або модернізації існуючих комплексів радіоконтролю. Запропоновані підходи забезпечують підвищення точності прогнозування ефективності систем виявлення джерел радіовипромінювання, оперативність та достовірність виявлення загроз. Це актуально у сучасних умовах, коли зростає використання короткочасних, хаотично розподілених у часі та частотному діапазоні сигналів, які важко піддаються виявленню стандартними засобами. Результати дослідження можуть бути корисні для фахівців у галузі технічного захисту інформації, при плануванні та організації заходів протидії несанкціонованому збиранню та передачі конфіденційної інформації.

Ключові слова: джерело радіовипромінювання; виявлення сигналу; електромагнітна доступність; ймовірність виявлення; надкороткі передачі; радіоконтроль; завадостійкість.



ВСТУП

Проблема захисту інформації від несанкціонованого доступу набуває особливої актуальності, важливу роль відіграє виявлення та нейтралізація технічних каналів витоку даних.

Одним із найпоширеніших способів негласного отримання конфіденційної інформації є використання засобів радіомоніторингу або джерел радіовипромінювання, які передають дані на відстань без візуального контакту. У зв'язку з цим ефективною протидією таким загрозам потребує розробки науково обґрунтованих методик оцінювання параметрів виявлення сигналів, що використовуються для незаконного отримання інформації.

Джерела радіовипромінювання можуть бути як постійно діючими, так і короткочасними, зокрема надкороткочасними, що значно ускладнює їхню реєстрацію та локалізацію. Особливу складність становить виявлення таких сигналів у умовах завад, високої щільності радіовипромінювань та обмеженої чутливості засобів радіоконтролю. Тому важливим є аналіз існуючих підходів до оцінки ефективності комплексів виявлення, а також розробка методики, яка дозволяла б прогнозувати ймовірність виявлення джерел радіовипромінювання в реальних умовах експлуатації.

Мета дослідження полягає у створенні та аналізі методики розрахунку ключових параметрів виявлення сигналів засобів негласного отримання інформації, зокрема джерел радіовипромінювання, з урахуванням часових, частотних та енергетичних характеристик. Такий підхід дає змогу забезпечити обґрунтування вибору технічних засобів радіоконтролю, оптимізацію їхніх параметрів, а також підвищення загальної ефективності систем протидії технічним каналам витоку інформації.

Робота спрямована на формування послідовного алгоритму оцінювання середнього часу виявлення джерела радіовипромінювання, ймовірності його розкриття за допустимий час спостереження, а також показників ефективності виявлення надкоротких передач. Запропоновані розрахункові вирази враховують широке коло факторів: тривалість випромінювання, діапазон частот, електромагнітну доступність, потужність сигналу на вході приймача, завади та шуми, характеристики антен та умов поширення радіохвиль.

Особливу увагу приділено питанням забезпечення електромагнітної доступності (ЕМД), яка є критичним фактором при виявленні слабких сигналів. Для цього запропоновано послідовність розрахунків, яка починається з обчислення потужності сигналу на вході приймача, врахування додаткового ослаблення радіохвиль, визначення рівня завад та порівняння знайдених значень із необхідними для виявлення. У разі невиконання умов ЕМД подано рекомендації щодо оптимізації параметрів приймальної апаратури або зміни умов її розташування.

Також розглянуто задачу визначення ймовірності частотно-часового контакту комплексу виявлення з джерелом випромінювання, що має особливе значення при виявленні надкоротких передач. Оцінка цього параметра здійснюється з урахуванням періоду перегляду діапазону частот, тривалості випромінювання, швидкості сканування та інших характеристик обладнання. Наведено формули для розрахунку ймовірності виявлення сигналів заданої тривалості, що дозволяє прогнозувати ефективність використання того чи іншого комплексу радіоконтролю в конкретних умовах.

Запропонована методика може бути використана як на етапі проектування систем радіоконтролю, так і для аналізу їхньої функціональної ефективності в процесі експлуатації. Вона забезпечує обґрунтування вибору технічних засобів, оптимізацію



режимів їх роботи та підвищує загальну ступінь захищеності інформації від несанкціонованого збирання та передачі.

Отже, проведення дослідження має практичне значення для фахівців у галузі інформаційної безпеки, радіоконтролю та технічного захисту інформації, оскільки дозволяє підвищити точність оцінки ефективності систем виявлення джерел радіовипромінювання та забезпечити більш високий рівень протидії технічним каналам витоку даних.

Постановка проблеми. Проблема захисту інформації від несанкціонованого доступу набуває особливого значення в умовах постійного технологічного розвитку. Одним із найпоширеніших способів нелегального збирання і передачі інформації є використання засобів радіомоніторингу або джерел радіовипромінювання, які передають дані на відстань без візуального контакту. Це створює загрозу технічного каналу витоку інформації, який важко виявити і нейтралізувати.

Особливо актуальною є задача виявлення короткочасних і надкоротких передач, які характеризуються малими часовими інтервалами випромінювання. Вони суттєво ускладнюють реєстрацію та локалізацію джерел через обмежений час взаємодії з системою виявлення.

Аналіз останніх досліджень і публікацій. Дослідження проблеми виявлення сигналів засобів негласного отримання інформації, зокрема джерел радіовипромінювання, має довгу наукову традицію, що відображена в численних працях вітчизняних і зарубіжних авторів.

Серед ключових напрямків наукових досліджень у цій галузі можна виділити аналіз електромагнітної доступності (ЕМД), оцінювання ймовірності виявлення короткочасних сигналів, розробку методик розрахунку середнього часу виявлення джерела радіовипромінювання та оптимізацію параметрів комплексів радіоконтролю.

У працях О.А. Лаптева, В.О. Хорошко, Кузавкова В.В. [1], В. П. Ільїна [2] та Ю. С. Шинкаренка [3] розглянуто теоретичні основи радіомоніторингу та технічні аспекти виявлення слабких сигналів на фоні завад. Ці автори акцентують увагу на важливості забезпечення електромагнітної доступності як одного з ключових факторів ефективності систем радіоконтролю.

У роботах [1] – [3] запропоновані моделі поширення радіохвиль у різних умовах, що дозволяють прогнозувати потужність сигналу на вході приймача, враховуючи такі параметри, як тип антен, відстань до джерела, характеристики фідерів, поляризація та ослаблення в середовищі поширення. Ці підходи були взяті за основу для побудови крокової методики розрахунку ЕМД, поданої в основному матеріалі.

Особливу увагу в літературі приділено питанням виявлення надкоротких передач, які є особливо складними для реєстрації через малий часовий інтервал випромінювання. У дослідженнях В. І. Борисова [4] та В. Г. Куліка [5] проаналізовано статистичні методи оцінювання ймовірності частотно-часового контакту комплексу виявлення з джерелом випромінювання. Автори розглядають вплив таких факторів, як тривалість сигналу, швидкість сканування діапазону частот, період перегляду діапазону та необхідний час на первинний технічний аналіз сигналу. Запропоновані формули для розрахунку ймовірності виявлення сигналів заданої тривалості.

Значний внесок у розвиток методології оцінювання ефективності систем радіоконтролю зробили дослідження, представлені в працях В. Г. Куліка [6] та О. І. Семенова [7]. Ці автори запропонували формалізовані алгоритми розрахунку середнього часу виявлення джерела радіовипромінювання, які враховують широке коло параметрів: діапазон спостереження, тривалість випромінювань, коефіцієнт розрідження вхідного



поток, реалізовану пропускну здатність підсистеми виявлення та ймовірність виявлення сигналу. Ці підходи безпосередньо використані в основному матеріалі обчислення середнього часу виявлення.

Важливим аспектом досліджень є аналіз впливу завад на ефективність виявлення сигналів. У працях В.О. Хорошко [8] та О.А. Лаптева [9] детально розглянуто способи оцінювання загальної потужності зовнішніх завад і внутрішніх шумів у різних діапазонах хвиль. Особливе значення приділено методам визначення допустимого ослаблення на шляху поширення сигналу та порівнянню його з реальним значенням для перевірки умов ЕМД. Системні підходи до проектування комплексів радіоконтролю розглянуті в працях С.П. Євсєєва [11] та В.В. Марченко [14]. Автори аналізують інтегровані системи, що об'єднують підсистеми пошуку, спостереження, розпізнавання та технічного аналізу сигналів. Особливої уваги заслуговує модель коефіцієнта розрідження вхідного потоку сигналів, який враховується при розрахунку ймовірності розкриття джерела радіовипромінювання за допустимий час.

Таким чином, літературні джерела, що стосуються теми дослідження, надають достатню наукову базу для розробки та аналізу методів оцінювання параметрів виявлення сигналів засобів негласного отримання інформації. Основний матеріал узагальнює та розвиває ці підходи, доповнюючи їх конкретними розрахунковими виразами, послідовністю кроків для визначення електромагнітної доступності, ймовірності виявлення та ефективності виявлення надкоротких передач.

Метою даної статті є підвищення точності прогнозування ефективності комплексів радіоконтролю, забезпечити оперативність та достовірність виявлення джерел радіовипромінювання, а також посилити захист інформації від несанкціонованого збирання та передачі через радіоканали.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Оцінювання середнього часу виявлення джерела радіовипромінювання.

Розрахунковий вираз для оцінювання часу розкриття джерела радіовипромінювань у загальному вигляді можна записати:

$$\bar{t}_{\text{роз}} = \frac{F_0 \cdot \lambda_f \cdot \bar{t}_{\text{он}}}{V \cdot \bar{t}_u \cdot \Lambda_p \cdot P_{\text{об}} \cdot P_{\text{он}}}, \quad (1)$$

де F_0 — діапазон частот спостереження і пошуку;

$\lambda_f = \frac{N_{\text{пу}}}{F_0}$ — питоме завантаження діапазону частот, що розвідується;

$\bar{t}_{\text{он}}$ — середній час, необхідний для виявлення джерела радіовипромінювання;

$\bar{t}_u$ — середня тривалість випромінювань;

V — коефіцієнт розрідження вхідного потоку підсистемами пошуку, спостереження і розпізнавання;

Λ_p — реалізована пропускну здатність підсистеми виявлення;

$P_{\text{он}}$ — ймовірність виявлення джерела радіовипромінювання;

$P_{\text{об}}$ — ймовірність виявлення сигналу комплексом радіоконтролю.

**Оцінювання імовірності розкриття джерела радіовипромінювання.**

Оцінювання імовірності розкриття джерела радіовипромінювання за час, що не перевищує припустимий, визначається виразом:

$$P(t_{\text{роз}} \leq T_0) = 1 - \exp\left[-\frac{\lambda}{V} \cdot P_{\text{об}} \cdot P_{\text{он}} \cdot T_0\right], \quad (2)$$

де T_0 — допустимий час ведення радіоспостереження;

V — коефіцієнт розрідження вхідного потоку підсистемами пошуку, спостереження і розпізнавання.

λ — інтенсивність надходження радіовипромінювань на комплекс радіоконтролю.

Оцінювання показників ефективності виявлення надкоротких передач.

Вихідні дані для розрахунку:

- імовірність забезпечення ЕМД (електромагнітна доступність) заданої якості ($P_{\text{ЕМД}}$);
- відстань до джерела радіовипромінювання;
- максимальне значення тривалості сигналів, що їх виявляють $t_{\text{випр}} \leq \lambda \cdot T_{\text{пр.м}}$
- потужність сигналу, джерела випромінювання (P_1);
- типи передавальної і приймальної антен і їхні параметри $G_1, G_2, \eta_{\phi 1,2}$, а також ступінь їхнього просторового узгодження ξ_n ;
- параметри приймача ($N_{\text{ш}}$ — коефіцієнт шуму, F_0 — діапазон огляду частот, γ — технічна швидкість сканування, $\square t_k$ — час, затрачуваний первинний технічний аналіз);
- тип середовища поширення радіохвиль.

Оцінювання можливості забезпечення електромагнітної доступності до джерела радіовипромінювання з заданою якістю.

Крок 1. Обчислюється потужність сигналу P_{co} на вході приймача.

$$P_{\text{co}} = P_1 + G_1 + G_2 + \eta_{\phi 1} + \eta_{\phi 2} + \xi_n + \xi_{\text{np}} + \xi_c + L_0 \left[\frac{\partial B}{Bm} \right], \quad (3)$$

де P_1 — потужність джерела випромінювання;

G_1, G_2 — коефіцієнт підсилення антен виявлення джерела випромінювання приймача;

$\eta_{\phi 1}, \eta_{\phi 2}$ — ККД передавального і приймального фідера;

ξ_n — коефіцієнт узгодження за поляризацією приймальної антени з полем хвилі, що приходить;

ξ_{np} — коефіцієнт просторового узгодження антен;

L_0 — згасання радіохвиль при поширенні у вільному просторі.

Крок 2. У залежності від умов і типу сфери поширення визначається додаткове ослаблення радіохвиль L_∂ .

Крок 3. Визначається потужність сигналу на вході комплексу виявлення:

$$P_{\text{с[об]}} = P_{\text{co}} + L_\partial. \quad (4)$$



Крок 4. За заданою імовірністю електромагнітної доступності $P_{EMД}$ визначається значення параметра x

$$x = \frac{\bar{Z} - Z_{mp}}{\sigma_z} = \Phi^{-1}(P_{EMД}). \quad (5)$$

Крок 5. Розраховується середнє перевищення рівня сигналу над рівнем завад - $\bar{Z}$:

$$\bar{Z} = Z_{mp} + x \cdot \sigma_z. \quad (6)$$

Крок 6. З огляду на те, що $h^2 = 10^{0,1\bar{Z}}$, при заданих технічних характеристиках джерела радіовипромінювання і пристрою приймання-виявлення знаходиться допустиме ослаблення на шляху L_∂ :

$$L_\partial = \frac{4h_0^2 k T_0 N_{ш} F_{ef}}{P_1 G_1 G_2}. \quad (7)$$

Крок 7. Для заданих довжини траси r , типу місцевості й умов пошуку (відкрита місцевість чи приміщення) обчислюється (аналітично чи графічно) реальне ослаблення на шляху — L_∂ .

Крок 8. Порівнюються реальне і допустиме ослаблення. Якщо $L_p < L_\partial$, то аргументу r дається збільшення $r = r + \Delta r$, і знову розраховується $L_p(r + \Delta r)$ для наступного порівняння.

Крок 9. Визначення $P_{ш}$, і потім $P_{сн}$.

На цьому кроці необхідно врахувати, що:

а) загальну потужність зовнішніх випадкових завад і внутрішніх шумів на вході приймача в діапазоні 30-100 МГц при $\eta_{AФТ} = 0,7 - 0,8$ і $\xi = 0,8$ можна вважати рівною:

$$P_{ш} = -(150 \div 160) + 10 \lg F_{e\Phi[\kappa\Gamma\zeta]} \left[\frac{\partial B}{Bm} \right]; \quad (8)$$

б) при проведенні розрахунків у діапазоні дециметрових і сантиметрових хвиль потужності завад на вході приймача приймаються рівними потужності його внутрішніх шумів:

$$P_{ш} = k T_0 N_{ш} F_{e\Phi[\kappa\Gamma\zeta]}, \quad (9)$$

де $k T_0 = 4 \cdot 10^{-18} \frac{Bm}{\kappa\Gamma\zeta}$; $N_{ш}$ - коефіцієнт шуму радіо приймального приймача.

Крок 10. Знаходиться мінімальне значення потужності сигналу на вході приймача, при якому забезпечується необхідна імовірність ЕМД (електромагнітна доступність) заданої якості:

$$P_{сн} = \bar{Z} + 101 \cdot \lg P_{ш}. \quad (10)$$



Крок 11. Порівнюються знайдені значення P_c і P_{CH} , з метою перевірки виконання умови забезпечення ЕМД:

а) якщо $P_c \geq P_{CH}$, то енергетична умова забезпечення електромагнітної доступності виконується;

б) якщо $P_c < P_{CH}$, то електромагнітна доступність при вибраних вихідних технічних параметрах виявника ($N_{ш}, G_2, \eta_{\phi 2}$) неможлива.

Крок 12. У випадку, якщо не є можливим забезпечити ЕМД заданої якості необхідно сформулювати обґрунтовані рекомендації з оптимального використання радіозасобів для зменшення чи повної компенсації недостатньої різниці між необхідним P_{CH} , і знайденим P_c , значеннями потужності сигналу $\Delta P = P_{CH} - P_c$.

Визначення ймовірності частотно-часового контакту комплексу виявлення з джерелом радіовипромінювання.

Крок 1. Якщо тривалість радіовипромінювання $t_{випр}$ не задана конкретно, то оцінка $\bar{T}_{випр} = \lambda \cdot T_{np.m}$, де $\lambda \in [0; 1]$ здійснюється методом імітаційного моделювання.

Крок 2. Період перегляду діапазону частот комплексом виявлення $\bar{T}$ для панорамного приймача й аналізатора спектра відомі і визначаються швидкістю розгортання, але для складних комплексів виявлення з підсистемою первинного аналізу сигналів значення періоду перегляду діапазону частот $\bar{T}$ варто визначати методом імітаційного моделювання на підставі виразу:

$$\bar{T} = T_{np.m} + \bar{N}_{pu} \cdot t_k, \quad (11)$$

де $T_{np.m}$ — час перегляду діапазону частот з технічною швидкістю аналізу (детермінована величина);

N_{pu} — кількість радіовипромінювань, з якими встановлюється контакт за частотою і часом за один прохід (випадкова величина, яка розподілена за законом Пуассона);

t_k — час, необхідний для первинного технічного аналізу.

Крок 3. Обчислення ймовірності частотно-часового контакту і випромінювання за один період перегляду досліджуваного діапазону частот:

$$P_K = \frac{\tau - 2t_K + t_u}{\bar{T}}, \text{ якщо } t_{випр} = const; \quad (12)$$

$$P_K = \frac{\tau - t_K}{\bar{T}} + \frac{t_u}{\bar{T}} \cdot \exp\left(-\frac{t_K}{t_u}\right) \left[1 - \exp\left(-\frac{T - \tau + t_K}{\bar{T}}\right)\right], \text{ якщо } t_{випр} = \lambda T_{np.m} \quad (13)$$

Імовірність виявлення надкоротких передач заданої тривалості $t_{випр}$ розраховується за формулою:

$$P_{об} = P_K \cdot P_C. \quad (14)$$

Тобто оцінювання ефективності виявлення коротких передач оцінюється імовірністю виявлення коротких передач та визначається за виразом (14).



ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У результаті проведеного дослідження розроблено та обґрунтовано методику оцінювання ключових параметрів виявлення сигналів засобів негласного отримання інформації, зокрема джерел радіовипромінювання. Запропоновані розрахункові вирази дозволяють прогнозувати середній час виявлення джерела, ймовірність його розкриття за допустимий час спостереження, а також ефективність виявлення надкоротких передач. Це забезпечує науково обґрунтований підхід до проектування систем радіоконтролю та аналізу їхньої функціональної ефективності в реальних умовах.

Особливу увагу приділено питанням забезпечення електромагнітної доступності, яка є критичним фактором при виявленні слабких сигналів на фоні завад. Розроблена послідовність розрахунків враховує такі параметри, як потужність сигналу на вході приймача, типи антен, їхнє просторове та поляризаційне узгодження, втрати в фідерах, умови поширення радіохвиль та додаткове ослаблення в залежності від місцевості. Порівняння реальної та необхідної потужності сигналу дозволяє перевірити виконання умов електромагнітної доступності і, у разі її невиконання, сформулювати рекомендації щодо оптимізації параметрів комплексу виявлення.

Також запропоновано методику визначення ймовірності частотно-часового контакту комплексу виявлення з джерелом радіовипромінювання, що має особливе значення при виявленні сигналів малої тривалості. Встановлено, що ефективність виявлення надкоротких передач суттєво залежить від швидкості сканування діапазону частот, періоду перегляду, тривалості сигналу та часу, необхідного для первинного технічного аналізу. Це дозволяє прогнозувати ймовірність виявлення сигналів заданої тривалості, що є важливим при проектуванні систем радіоконтролю.

Отримані результати можуть бути використані як при проектуванні нових, так і при модернізації існуючих комплексів радіоконтролю. Вони дають змогу обґрунтовано вибирати технічні засоби, оптимізовувати режими їхньої роботи, а також підвищити загальну ефективність протидії технічним каналам витоку інформації. Особливо це актуально у умовах зростаючого використання короткочасних, хаотично розподілених у часі та частотному діапазоні сигналів, які важко піддаються виявленню стандартними засобами.

Таким чином, представлені у статті методики розрахунку параметрів виявлення сигналів дозволяють підвищити точність прогнозування ефективності комплексів радіоконтролю, забезпечити оперативність та достовірність виявлення джерел радіовипромінювання, а також забезпечити більш високий рівень захисту інформації від несанкціонованого збирання та передачі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Laptev, O.A., Kuzavkov, V.V., & Khoroshko, V.O. (2023). *Textbook "Search systems for covert acoustic information acquisition"*. Kyiv: Millennium.
2. Ilyin, V.P. (2012). *Technical means of radio control*. Kharkiv: KHVU.
3. Shynkarenko, Y.S. (2014). *Electromagnetic compatibility and availability*. Odesa: Nauka.
4. Borisov, V. I. (2011). *Statistical methods of signal analysis*. Kyiv: Naukova Dumka.
5. Kulyk, V.G. (2009). *Methods for evaluating the effectiveness of radio control*. Kyiv: Publishing house "Politehnika".
6. Semenov, O.I. (2015). *Formalized models of radio interference*. Kharkiv: KNURE.



7. Laptev, O.A., & Khoroshko, V.O. (2024). *Detection, localization and processing of signals of covert information gathering equipment*. Kyiv: Millennium.
8. Barabash, O.V., Laptev, A.A., Svynchuk, O.V., Solovyov, E.V., & Bushkov, V.G. (2020). Estimation of the noise immunity of the radio signal detection path. *Modern Information Protection*, 1, 18–24.
9. Laptev, O.A., Sobchuk, V.V., & Savchenko, V.A. (2019). A method for increasing the noise immunity of the system for detecting, recognizing and localizing digital signals in information systems. *Collection of scientific papers of the Military Institute of Taras Shevchenko National University of Kyiv. VIKNYK*, 66, 124–132.
10. Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O., Korol, O., & Milevskyi, S. et. al. (2023). *Models of socio-cyber-physical systems security: Monographs*. PC TECHNOLOGY CENTER. <http://doi.org/10.15587/978-617-7319-72-5>
11. Laptiev, O., Sobchuk, V., Ryzhov, A., Sobchuk, A., Kopytko, S. & Shuklin, G. (2024). Harmonic Operators in Mathematical Models of Sources of Detection of Unauthorized Access to Information. *6 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA 2024)*, 1–6. <https://doi.org/10.1109/HORA61326.2024.10550552>
12. Laptev, O., Sobchuk, V., Barabash, O., & Musienko, A. (2022). A method for determining the parameters of radio-embedded devices using differential transforms. *V International scientific and practical conference. "Problems of cybersecurity of information and telecommunication systems" (PCSITS)*, 63–65.
13. Laptev, O.A., & Marchenko, V.V. (2025). Application of interference to protect information from leakage by radio channel. *Modern information protection*, 1, 89–97. <https://doi.org/10.31673/2409-7292.2025.013057>

**Oleksandr Laptiev**

Doctor of Technical Science, Senior Researcher
Associate Professor the Department of Cyber Security and Information Protection
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID ID: 0000-0002-4194-402X
olaptiev@knu.ua

Tetiana Laptieva

PhD in Cybersecurity
State University of Trade and Economics
ORCID ID: 0000-0002-5223-9078
tetiana1986@ukr.net

Mykola Brailovskyi

PhD, Associate Professor at the Department
Department of Cybersecurity and Information Protection
Taras Shevchenko National University of Kiev
Bohdan Havrylyshyn Str., 24, Kyiv, Ukraine, 04116
Kiev, Ukraine
ORCID ID: 0000-0002-3148-1148
bk1972@ukr.net

METHODS FOR ASSESSING INFORMATION SECURITY IN COMMUNICATION NETWORKS

Abstract. The article considers methods for evaluating the parameters of detecting signals of means of covert information acquisition, in particular sources of radio radiation. Calculation expressions are given for determining the average time of detection of a source of radio radiation and the probability of its disclosure during the permissible observation time. Special attention is paid to assessing the efficiency of detecting ultrashort transmissions, which are characterized by small time intervals of radiation. For this purpose, a sequence of calculations is proposed, which includes the analysis of electromagnetic accessibility, determination of the signal power at the receiver input, taking into account interference and noise, as well as calculating the probability of frequency-time contact of the detection complex with the radiation source. The main factors affecting the detection efficiency are considered: radiation duration, frequency range, technical characteristics of the receiving equipment, radio wave propagation conditions and interference conditions. An approach is proposed to determine the required sensitivity of radio control means to ensure a given probability of detection. Recommendations are also given for optimizing the parameters of the detection system in case of failure to meet the conditions of electromagnetic accessibility. The methodology can be used in the design of radio control complexes, as well as for the analysis of their effectiveness in real operating conditions. The results obtained allow to increase the accuracy of the assessment of the capabilities of systems for detecting radio radiation sources and to ensure effective counteraction to technical channels of information leakage.

Keywords: radio emission source; signal detection; electromagnetic accessibility; detection probability; ultrashort transmissions; radio control; interference immunity.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Laptev, O.A., Kuzavkov, V.V., & Khoroshko, V.O. (2023). *Textbook "Search systems for covert acoustic information acquisition"*. Kyiv: Millennium.
2. Ilyin, V.P. (2012). *Technical means of radio control*. Kharkiv: KHVU.
3. Shynkarenko, Y.S. (2014). *Electromagnetic compatibility and availability*. Odesa: Nauka.
4. Borisov, V. I. (2011). *Statistical methods of signal analysis*. Kyiv: Naukova Dumka.
5. Kulyk, V.G. (2009). *Methods for evaluating the effectiveness of radio control*. Kyiv: Publishing house "Politehnika".



6. Semenov, O.I. (2015). *Formalized models of radio interference*. Kharkiv: KNURE.
7. Laptev, O.A., & Khoroshko, V.O. (2024). *Detection, localization and processing of signals of covert information gathering equipment*. Kyiv: Millennium.
8. Barabash, O.V., Laptev, A.A., Svynchuk, O.V., Solovyov, E.V., & Bushkov, V.G. (2020). Estimation of the noise immunity of the radio signal detection path. *Modern Information Protection*, 1, 18–24.
9. Laptev, O.A., Sobchuk, V.V., & Savchenko, V.A. (2019). A method for increasing the noise immunity of the system for detecting, recognizing and localizing digital signals in information systems. *Collection of scientific papers of the Military Institute of Taras Shevchenko National University of Kyiv. VIKNYK*, 66, 124–132.
10. Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O., Korol, O., & Milevskyi, S. et. al. (2023). *Models of socio-cyber-physical systems security: Monographs*. PC TECHNOLOGY CENTER. <http://doi.org/10.15587/978-617-7319-72-5>
11. Laptiev, O., Sobchuk, V., Ryzhov, A., Sobchuk, A., Kopytko, S. & Shuklin, G. (2024). Harmonic Operators in Mathematical Models of Sources of Detection of Unauthorized Access to Information. *6 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA 2024)*, 1–6. <https://doi.org/10.1109/HORA61326.2024.10550552>
12. Laptev, O., Sobchuk, V., Barabash, O., & Musienko, A. (2022). A method for determining the parameters of radio-embedded devices using differential transforms. *V International scientific and practical conference. "Problems of cybersecurity of information and telecommunication systems" (PCSITS)*, 63–65.
13. Laptev, O.A., & Marchenko, V.V. (2025). Application of interference to protect information from leakage by radio channel. *Modern information protection*, 1, 89–97. <https://doi.org/10.31673/2409-7292.2025.013057>

