УДК 004.056.53 DOI: 10.31673/2518-7678.2021.011926

Шуклін Г.В., к.т.н.; **Пепа Ю.В.,** к.т.н.;
Науменко А.В., аспірант; **Лазебний В.А.,** аспірант

ВИЗНАЧЕННЯ ЗАКОНУ РОЗПОДІЛУ ЙМОВІРНОСТІ УСПІШНОГО НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В СИСТЕМІ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ НАЯВНОСТІ ПАРАМЕТРИЧНОЇ НЕВИЗНАЧЕНОСТІ

Shuklin G.V., Pepa Y.V., Naumenko A.V., Lazebniy V.A. Determination of law of distribution of probability of successful unauthorized division to confidential information in the system of defence of information at presence of self-reactance vagueness. In-process it offers to use ortogonal rows for the construction of laws of probability distribution in the models of defence of information at presence of self-reactance vagueness. Adequacy of method is determined long ortogonal row on the basis of the data got by means of supervisions of presence of unauthorized attempt to get confidential information on the object of informative activity. The aim of the article is a receipt of estimation of unknown function of distribution of probability of successful unauthorized removal of confidential information in the conditions of self-reactance vagueness. As a result, the algorithm of construction of ortogonal rows is in-process presented for determination of estimation of laws of distribution of probability of successful realization of unauthorized removal of confidential information on the objects of informative activity in the conditions of self-reactance vagueness. On the example of radio frequency channel of information transfer the estimation of probability of successful removal of confidential information was practically carried out on an object of informative activity, that was determined as dependence of relation of exceeding of level of amplitude of informing signal to the thresholding on the basis of supervisions that was taken off in laboratory terms by means of oscillograph and comparator on the basis of integral microcircuit of LM339 of company Motorola. As a conclusion, the use of ortogonal rows is in-process shown for the estimation of closeness of distribution of probability of successful unauthorized removal of confidential information on the object of informative activity in the conditions of parametric vagueness on the example of radio frequency channel. It is noticed, that this algorithm is comfortable and informing, if a closeness of distribution of probability is a function from the small amount of variables(not more than three). In case if the function of distribution of probability has a dimension more than three, then this algorithm becomes difficult in connection with complication of construction of ortogonal rows.

Шуклін Г.В., Пепа Ю.В., Науменко А.В., Лазебний В.А. Визначення закону розподілу ймовірності успішного несанкціонованого доступу до конфіденційної інформації в системі захисту інформації при наявності параметричної невизначеності. В роботі запропоновано використовувати ортогональні ряди для побудови законів розподілу ймовірностей в моделях захисту інформації при наявності параметричної невизначеності. Адекватність методу визначається довжиною ортогонального ряду на основі даних, отриманих за допомогою спостережень наявності несанкціонованої спроби отримати конфіденційну інформацію на об'єкті інформаційної діяльності.

Шуклин Г.В., Пепа Ю.В., Науменко А.В., Лазебный В.А. Определение закона распределения вероятности успешного несанкционированного доступа до конфиденциальной информации в системе защиты информации при наличии параметрической неопределённости. В работе предложено использовать ортогональные ряды для построения законов распределения вероятностей в моделях защиты информации при наличии параметрической неопределённости. Адекватность метода определяется длиной ортогонального ряда на основе данных, полученных с помощью наблюдений наличия несанкционированной попытки получить конфиденциальную информацию на объекте информационной деяльности.

Вступ

Постановка задачі. Процес пошукової ідентифікації полягає в налаштовуванні параметрів однієї або декількох моделей, визначення критеріїв ідентифікації і відповідних функцій якості, і оцінювання за цією інформацією значення ідентифікованого параметра.

В задачах виявлення закладних пристроїв, які є засобами негласного отримання інформації, важливим є в першу чергу виявлення місць в приміщенні, де вони реально можуть бути сховані. При візуальному огляді приміщення не завжди можна швидко це зробити. Тому задача введення необхідного параметру, за допомогою якого можна ідентифікувати місце можливого знаходження засобу негласного отримання інформації є актуальною і потребує ретельного вивчення.

Аналіз літературних джерел. В класичних моделях теорії керування визначаються параметри, які характеризують параметричну невизначеність [1]. Наслідком неможливості безпосереднього використання вихідних сигналів об'єкта і моделей в якості критерію ідентифікації призводить до того, що для отримання оцінки критерію, як правило, потрібно чимало часу [2] і процедура суттєво ускладнюється. Одним із способів подолання зазначеної проблеми, є використання ортогональних базисів [3] якими можна описати випадкові процеси успішного перехоплення інформації. Але їх вибір не є простим, так як саме від виду базисних функцій буде залежати простота чи складність отримання закону розподілу перехопленої інформації, що в подальшому вплине на вибір одного з оптимальних критеріїв [4]. Тому базисна функція і буде тією основою, яка дозволить математично описати систему перехоплення інформації за фактично відсутніми апріорними данними, тобто в умовах невизначеності. Саме застосовуючі певні обмеження (параметри) до базисних функцій дозволить в подальшому виявити моменти перехоплення інформації і проаналізувати їх.

Мета та задачі дослідження. Отримання оцінки невідомої функції розподілу ймовірності успішного несанкціонованого зняття конфіденційної інформації в умовах параметричної невизначеності.

Викладення основного матеріалу

В основі побудови оцінки невідомої функції розподілу ймовірності успішного несанкціонованого зняття конфіденційної інформації на об'єкті інформаційної діяльності лежить проекційне наближення. Сутність цього наближення полягає в тому, що якщо деяка неперервна функція $f(\eta)$ визначена на деякому інтервалі $[-\tau;\tau]$ і для кожної невід'ємної на цьому інтервалі функції $g_i(\eta)$, виконується умова:

$$\forall i \neq j : \int_{-\tau}^{\tau} g_i(\eta) g_j(\eta) d\eta = 0 \ , \ i = 1,2,... \ , \tag{1}$$

і при цьому інтеграл $\int_{-\tau}^{\tau} f^2(\eta) g_i(\eta) d\eta$ збігається, то функцію $f(\eta)$ можна представити у вигляді:

$$f(\eta) = \lim_{n\to\infty} \sum_{i=1}^{n} b_i g_i(\eta) \, . \tag{2}$$

Використовуючи умову (1) і представлення (2) можна здійснювати оцінку закону розподілу успішної реалізації несанкціонованого зняття конфіденційної інформації на об'єктах інформаційної діяльності. В якості системи функцій $\{ g_i(\eta) \}$, $i = 1,2,...$ при дослідженні моделюванні захисту конфіденційної інформації на об'єктах інформаційної діяльності зручно вибирати наступну систему:

$$\{0{,}5; e^{-k|\eta|}; \sin(\pi k \eta)\} \, , \ k = 1,2,... \ . \tag{3}$$

Для системи функцій (3) виконується умова (1) і тоді проекційна оцінка (2) прийме вид

$$\overline{p_n}(\eta) = 0{,}5 + \lim_{n\to\infty} \left(\sum_{k=1}^{n} \left(a_k e^{-k|\eta|} + \sin(\pi k \eta) \right) \right) . \tag{4}$$

Визначення коефіцієнтів a_k в розкладі (4) є достатньо складною задачею і в першу чергу необхідно виконання умови нормування

$$\int_{-\lambda}^{\lambda}\left(0{,}5+\lim_{n\to\infty}\left(\sum_{k=1}^{n}\left(a_k e^{-k|\eta|}+\sin(\pi k\eta)\right)\right)\right)=1,$$

звідки отримуємо:

$$\lim_{n\to\infty}\sum_{k=1}^{n}\frac{a_k}{k}\left(1-e^{-k|\eta|}\right)=0{,}5. \tag{5}$$

Так як $\lim_{n\to\infty} e^{-k|\eta|}=0$, а кількість доданків в реальних дослідженнях має скінченне число, то цим рівність (5) можна замінити на рівність:

$$\sum_{k=1}^{n}\frac{a_k}{k}=0{,}5. \tag{6}$$

З рівності (6) виникає необхідність в визначенні найменшого числа n, щоб при умові отримати достовірний закон розподілу ймовірності (4) успішної реалізації несанкціонованого зняття конфіденційної інформації на об'єкті інформаційної діяльності. Визначення кількості доданків, яких достатньо для виконання рівності (6) визначається самими властивостями об'єкта інформаційної діяльності, а також залежить від того, чи несанкціоноване зняття конфіденційної відбувається закладними засобами, які заховані на об'єкті, чи приймачами, які знаходяться за межами приміщення.

При дослідженні об'єкта інформаційної діяльності на можливість здійснення несанкціонованого доступу до конфіденційної інформації приміщення U розбивають на зони, які не перетинаються і $U=\bigcup_{i=1}^{n}U_i$ і кожну зону U_i приміщення ретельно перевіряють на наявність закладних пристроїв (рис.1).

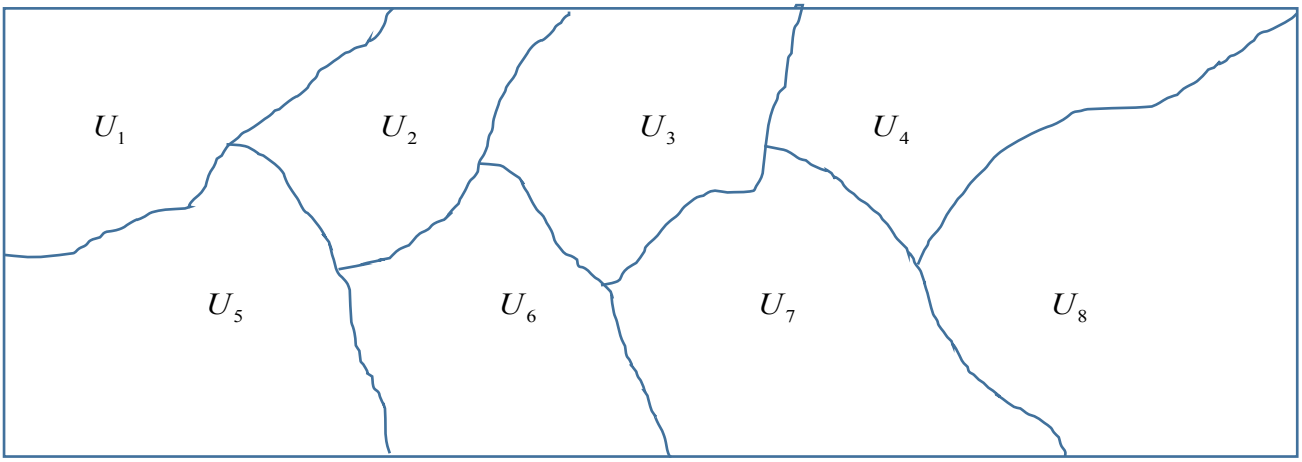

Рис. 1. Приклад розбиття приміщення об'єкта інформаційної діяльності на зони, що не перетинаються

Кожна з зон має свою площу S_{U_i} В цьому випадку первинну ймовірність наявності засобу негласного зняття інформації можна визначити як:

$$p_i=\frac{S_{U_i}}{S}, \tag{7}$$

де S_i - площа i - ї зони U_i (наприклад частина підлоги, або стіни), а S - площа всієї області приміщення. Тоді кількість доданків в представлені (5) визначається кількістю областей на які було поділено приміщення об'єкта інформаційної діяльності. Однак, при дослідження кожної зони на наявність закладних пристроїв дане розбиття може змінюватись,

а значить і кількість доданків в рівності (6) також буде змінюватись. В даній роботі припускається, що розбиття приміщення на зони не змінюється і в залежності від того, за яким фізичним принципом працює прилад, за допомогою якого здійснюється пошук закладного пристрою вводиться параметр η, який і визначає можливе знаходження засобу негласного зняття інформації в той чи іншій зоні. Тоді, в представлені (7) ймовірність p_i стає функцією від цього параметру, тобто $p_i = p_i(\eta)$. Використовуючи метод найменших квадратів визначається критерій, за яким визначаються коефіцієнти a_k в представлені (4):

$$F = \left(0{,}5 + \lim_{n\to\infty} \sum_{k=1}^{n} \left(a_k e^{-k|\eta_i|} + \sin(\pi k \eta_i) \right) - p_i \right)^2 \to \min . \qquad (8)$$

На прикладі радіочастотного каналу передачі інформації в лабораторних умовах за допомогою осцилографа та компаратора на основі інтегральної мікросхеми LM339 компанії Motorola було проведено дослідження на предмет наявності радіо закладного пристрою, в той чи іншій зоні об'єкта інформаційної діяльності. Припускалось, що пороговий рівень сигналу складає ± 50 дБ і головний параметр λ, який визначав можливу наявність закладного пристрою в зоні є різниця між дійсним рівнем сигналу і пороговим його значенням. Приміщення загальною площею 64 квадратних метри було розділено на чотири зони, площі яких: $S_{U_1} = 16$ кв. м. , $S_{U_2} = 20$ кв. м., $S_{U_3} = 15$ кв. м., $S_{U_4} = 13$ кв. м. Результати досліду представлено в таблиці 1.

Таблиця 1

Числові значення визначення рівня сигналу на об'єкті інформаційної діяльності, який було поділено на чотири зони

Час в секундах запису в комірку пам'яті осцилографа миттєвого значення напруги на виході радіоприймача	**Рівень сигналу r_i в дБ (децибелах)**	**Порогове значення рівня сигналу r_n в дБ (децибелах)**	$\lambda_i = r_i - r_n$	**Зона**	$p_i = \frac{S_{Ui}}{S}$
0,5	-76	-50	-26	U_1	0,25
1	-74,2	-50	-24,2	U_1	0,25
1,5	12	50	-38	U_4	0,203125
2	0,5	50	-49,5	U_2	0,3125
2,5	-32,5	-50	17,5	U_3	0,234375
3	-42,1	-50	8	U_1	0.25
3,5	62,5	50	12,5	U_3	0,234375
4	64	50	14	U_1	0,25
4,5	11,5	50	-38,5	U_4	0,203125
5	2,5	50	-47,5	U_2	0,3125
5,5	-7	-50	43	U_2	0,3125
6	-8,2	-50	41,8	U_2	0,3125
6,5	63	50	13	U_1	0,25
7	42,5	50	-7,5	U_3	0,234375
7,5	4	50	-46	U_2	0,3125
8	-16,5	-50	33,5	U_4	0,203125
8,5	22	50	-28	U_4	0,203125

Продовження таблиці 1

Числові значення визначення рівня сигналу на об'єкті інформаційної діяльності, який було поділено на чотири зони

Час в секундах запису в комірку пам'яті осцилографа миттєвого значення напруги на виході радіоприймача	**Рівень сигналу r_i в дБ (децибелах)**	**Порогове значення рівня сигналу r_n в дБ (децибелах)**	$\lambda_i = r_i - r_n$	**Зона**	$p_i = \frac{S_{U_i}}{S}$
9	38,5	50	-7,5	U_4	0,203125
9,5	11	50	-39	U_2	0,3125
10	3	50	-47	U_2	0,3125
10,5	-0,5	-50	49,5	U_2	0.3125
11	61,5	50	11,5	U_1	0,25
11,5	42	50	-8	U_3	0,234375
12	-36	-50	14	U_3	0,234375
12,5	-42,5	-50	7,5	U_3	0,234375
13	-1,5	-50	48,5	U_2	0,3125
13,5	60	50	10	U_1	0,25
14	-0,5	-50	49,5	U_2	0,3125
14,5	33,5	50	-16,5	U_4	0,203125
15	38,5	50	-11,5	U_4	0,203125
15,5	14,5	50	-35,5	U_3	0,234375
16	8,2	50	-31,8	U_2	0,3125
16,5	-11	-50	39	U_2	0,3125
17	2,5	50	-47,5	U_2	0,3125
17,5	62,2	50	12,2	U_1	0,25
18	-31	-50	19	U_3	0,234375
18,5	-12,5	-50	31,5	U_3	0,234375
19	5,5	50	-44,5	U_2	0,3125
19,5	26,5	50	-23,5	U_3	0,234375
20	-33	-50	17	U_3	0,234375
21	18,5	50	-31,5	U_3	0,234375
21,5	38	50	-12	U_3	0,234375
22	62	50	12	U_1	0,25
22,5	22	50	-28	U_3	0,234375
23	6,2	50	-53,8	U_2	0,3125
23,5	-14,5	-50	35,5	U_2	0,3125
24	-52	-50	2	U_1	0,25
24,5	2,5	50	-47,5	U_2	0,3125
25	-2,5	-50	47,5	U_2	0,3125
25,5	8	50	-52	U_2	0,3125

Якщо при пороговому значенні рівня сигналу в – 50 дБ значення параметру λ_i приймав додатне значення, або при пороговому значенні рівня сигналу в 50 дБ цей параметр приймав від'ємне значення, то це означало, що в даній зоні є підозра про наявність закладного пристрою і необхідно вже досліджувати ці зони приміщення. При проведеному досліді, було встановлено, що якщо в приміщення сховано засіб негласного зняття інформації, то він знаходився в зоні U_1, а всі інші три зони відпадають, так як в них рівень сигналу при проведених дослідах не виходив за порогові.

На рисунку 2 представлено миттєве значення рівня сигналу на виході радіоприймача в один з моментів часу.

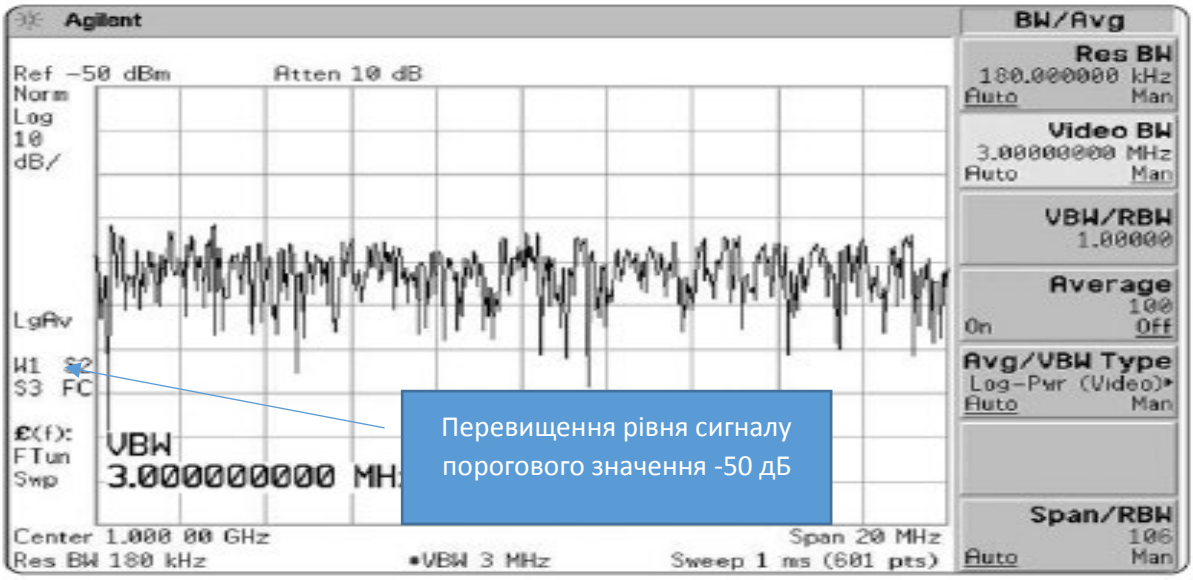

Рис. 2. Миттєве значення рівня сигналу на виході радіоприймача в момент часу $t = 1$ с

Рисунок 2 показує, що в даний момент часу було зафіксовано перевищення рівня сигналу в зоні U_1. При пороговому значення рівня сигналу в -50дБ було зафіксовано рівень сигналу в -74,2 дБ.

Так як було виявлено тільки одну зону приміщення, де можливо знаходився закладний пристрій, то в представлені (5) кількість доданків дорівнює кількості перевищень рівня сигналу. В таблиці 2 представлено значення відношення цих перевищень до порогового і час запису в комірку осцилографа в який це перевищення було зафіксовано.

Таблиця 2

Значення перевищень рівня сигналу від порогового значення

Час фіксації	0,5	1	3,5	4	6,5	11	13,5	17,5	22	24
$\eta_i = \frac{}{}$	0,52	0,484	0,25	0,28	0,26	0,23	0,2	0,244	0,24	0,04
p_i	0,4	0,4	0,35	0,38	0,4	0,34	0,3	0,35	0,35	0,09

При практичному досвіді виявлення закладних пристроїв достатньо взяти два доданки в представлені (4). Тоді, використовуючи критерій (8) і дані таблиці 2, маємо:

$$F = \left(0{,}31 + a_1 e^{-0{,}52} + \sin 0{,}52\pi + a_2 e^{-1{,}04} + \sin 1{,}04\pi\right)^2 +$$

$$+\left(0{,}32+a_1e^{-0{,}484}+\sin 0{,}484\pi+a_2e^{-0{,}968}+\sin 0{,}968\pi\right)^2+$$
$$+\left(0{,}41+a_1e^{-0{,}25}+\sin 0{,}25\pi+a_2e^{-0{,}5}+\sin 0{,}5\pi\right)^2+$$
$$+\left(0{,}4+a_1e^{-0{,}28}+\sin 0{,}28\pi+a_2e^{-0{,}56}+\sin 0{,}56\pi\right)^2+$$
$$+\left(0{,}4+a_1e^{-0{,}26}+\sin 0{,}26\pi+a_2e^{-0{,}52}+\sin 0{,}52\pi\right)^2+$$
$$\left(0{,}42+a_1e^{-0{,}23}+\sin 0{,}23\pi+a_2e^{-0{,}46}+\sin 0{,}46\pi\right)^2+\left(0{,}43+a_1e^{-0{,}2}+\sin 0{,}2\pi+a_2e^{-0{,}4}+\sin 0{,}4\pi\right)^2+$$
$$\left(0{,}41+a_1e^{-0{,}244}+\sin 0{,}244\pi+a_2e^{-0{,}488}+\sin 0{,}488\pi\right)^2+$$
$$+\left(0{,}41+a_1e^{-0{,}24}+\sin 0{,}24\pi+a_2e^{-0{,}48}+\sin 0{,}48\pi\right)^2+$$
$$\left(0{,}49+a_1e^{-0{,}04}+\sin 0{,}04\pi+a_2e^{-0{,}08}+\sin 0{,}08\pi\right)^2\to\min.$$

З урахуванням умови нормування (6), розв'язуючи систему рівнянь:

$$\begin{cases}\dfrac{\partial F}{\partial a_1}=0\\[2ex]\dfrac{\partial F}{\partial a_2}=0\\[2ex]\displaystyle\int_0^1\left(0{,}5+\xi+a_1e^{-\eta}+\sin\pi\eta+a_2e^{-2\eta}+\sin 2\pi\eta\right)d\eta=1\end{cases},$$

отримуємо $a_1=1{,}569$, $a_2=-2{,}119$. Тоді закон розподілу ймовірності успішного зняття конфіденційної інформації в проведенному досліджені прийме вид:

$$\overline{p_2}(\eta)=0{,}6+1{,}569e^{-|\eta|}+\sin\pi\eta-2{,}119e^{-2|\eta|}+\sin 2\pi\eta. \qquad (10)$$

На рисунку 1 зображено графік функції розподілу (10).

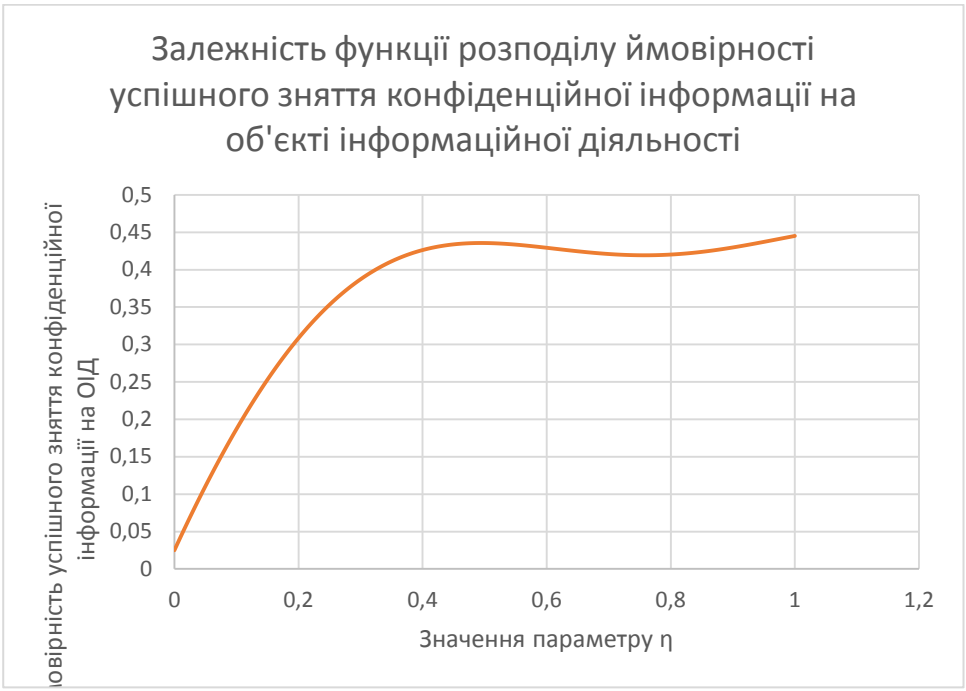

Рис. 2. Залежність функції розподілу ймовірності успішного зняття конфіденційної інформації від успішного зняття конфіденційної інформації

Висновки

В роботі продемонстровано використання ортогональних рядів для оцінки щільності розподілу ймовірності успішного несанкціонованого зняття конфіденційної інформації на

об'єкті інформаційної діяльності в умовах непараметричної невизначеності на прикладі радіочастотного каналу. Можливість отримання даної щільності розподілу дає спроможність виявляти місця на об'єкті інформаційної діяльності, де з достатньо точною ймовірністю можна виявляти засоби негласного зняття конфіденційної інформації. Підмічено, що даний алгоритм є зручним та інформативним, якщо щільність розподілу ймовірності є функцією від невеликої кількості змінних (не більше трьох). У випадку, якщо функція розподілу ймовірності має розмірність більше трьох, то даний алгоритм стає складним у зв'язку зі складністю побудови ортогональних рядів.

Список використаної літератури

1. Никифоров В.О., Слита О.В., Ушаков А.В. Интеллектуальное управление в условиях неопределенности / . – СПб: СПбГУ ИТМО, 2009. – 232 с.

2. Гуда А.И., Михалев А.И. Информационные оценки сложности задачи параметрической идентификации динамических систем // Адаптивні системи автоматичного управління. Міжвідом. наук.-техн. зб. праць (РИНЦ). – Днепропетровск, 2007. – 10(30). – С.96-103.

3. Ahmed N., Rao K.R. Orthogonal Transforms for Digital Signal Processing. – New York: Springer-Verlag, 1975. – PP. 264.

4. Akcay H., Ninness B. Orthonormal Basis Functions for Modelling Continuous-time Systems // Signal Processing. – Vol. 77. – Issue 3, 1999. – P.261-274.

5. Барабаш О.В., Лаптєв О.А., Мусієнко А.П., Собчук В.В. Методика виявлення несанкціонованого доступу до інформаційних систем підприємства у цифровому діапазоні // Зв'язок. 2019, №1. – С. 3-7.

6. Лаптєв О.А., Шуклін Г.В., Савченко В.А. Метод оцінювання параметрів імпульсного сигналу на основі кореляційно-регресійного аналізу // Зв'язок. 2019, №2. – С. 23-27.

Автори статті

Шуклін Герман Вікторович – кандидат технічних наук, доцент, завідуючий кафедрою Систем інформаційного та кібернетичного захисту, Державний університет телекомунікацій, Київ, Україна.

Пепа Юрій Володимирович – кандидат технічних наук, доцент, доцент кафедри Систем інформаційного та кібернетичного захисту, Державний університет телекомунікацій, Київ, Україна.

Науменко Антон Володимирович – аспірант, Державний університет телекомунікацій, Київ, Україна.

Лазебний Владіслав Анатолійович – магістр, Державний університет телекомунікацій, Київ, Україна.

Authors of the article

Shuklin Herman Viktorovych – candidate of Science (technic), assistant professor, head of Department of Information and cyber security, State University of Telecommunications, Kyiv, Ukraine.

Pepa Yurii Volodymyrovych – candidate of Science (technic), assistant professor, assistant professor of Department of Information and cyber security, State University of Telecommunications, Kyiv, Ukraine.

Naumenko Anton Volodymyrovych – postgraduate, State University of Telecommunications, Kyiv, Ukraine.

Lazebnyi Vladislav Anatoliiovych – master of Science, State University of Telecommunications, Kyiv, Ukraine.

Дата надходження в редакцію 12.10.2021 р. Рецензент: д.т.н., професор К.П. Сторчак