УДК 004.056.53:519.226 DOI: 10.31673/2412-4338.2024.019505

Половінкін Микола Ігорович
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0009-0009-5242-567X

Глухов Сергій Іванович
Київський національний університет імені Тараса Шевченка, Київ
ORCID 0000-0002-4918-3739

Черній Дмитро Іванович
Київський національний університет імені Тараса Шевченка, Київ
ORCID 0000-0002-6378-8048

Пархоменко Іван Іванович
Київський національний університет імені Тараса Шевченка, Київ
ORCID 0000-0001-6889-9284

АЛГОРИТМ ВИЯВЛЕННЯ ВИТОКУ ІНФОРМАЦІЇ НА ОСНОВІ ПЕРЕВІРКИ СТАТИСТИЧНИХ ГІПОТЕЗ

Анотація. *Для успішного виконання наукових досліджень, сучасні умови вимагають застосування різноманітних моделей та методів. Одним з варіантів можливо використовувати наукові методидля котрих потрібно саме розв'язання задач в умовах наявності невизначеностей. Відмінністю методів байєсівського аналізу даних є те, що вони не вимагають наявності значних об'ємів даних, на яких можна було б побудувати необхідні моделі для їх подальшого використання. Фактично, цей метод може ґрунтуватись на коротких вибірках, на експертних оцінках, окремих вимірах, що є саме обґрунтовує використання його для виявлення випадкових сигналів радіомоніторингу. Запропоновано алгоритм виявлення та розпізнавання сигналів засобів негласного отримання інформації на основі перевірки статистичних гіпотез. Проведено математичне моделювання двох випадків перший апріорний розподіл параметру сигналу рівномірний та другій випадок коли апріорний розподіл параметра нормальний розподілу. Математичні розрахунки показали можливість використання теореми Байєса для побудови алгоритму виявлення та розпізнавання сигналів засобів негласного отримання інформації. Доведено, що у випадку, коли вибіркове середнє має нормальний розподіл і відомою дисперсією, а імовірність має нормальний розподіл, то апостеріорний розподіл для імовірності також нормальний. Обчислення підтвердили переваги другого випадку, в якому дисперсія апостеріорного розподілу зменшилась з 2,0 до 0,25. Це призвело до скорочення невизначеності розподілу завдяки отриманим даним після радіомоніторингу. Саме це дало можливість застосувати теорему Байєса для виявлення та розпізнавання сигналів засобів негласного отримання інформації, а також перевірити адекватність запропонованого алгоритму.*

Ключові слова: *теорема Байєса, персональні дані, особиста інформація, гіпотеза, випадковий сигнал, метод, неправдива інформація, кластерізація.*

UDC 004.056

Polovinkin Mykola
State university information and communication technologies Kyiv
ORCID 0009-0009-5242-567X

Glukhov Sergey
Taras Shevchenko national university Kyiv
ORCID 0000-0002-4918-3739

Cherniy Dmytro
Taras Shevchenko national university Kyiv
ORCID 0000-0002-6378-8048

Parkhomenko Ivan
Taras Shevchenko national university Kyiv
ORCID 0000-0001-6889-9284

INFORMATION LEAKAGE DETECTION ALGORITHM BASED ON CHECKS OF STATISTICAL HYPOTHESES

Abstract. *The successful implementation of modern research requires the use of a wide variety of methods that can be used to solve problems in the presence of uncertainties. The difference between Bayesian data analysis methods is that they do not require the availability of significant volumes of data on which the necessary models can be built for their further use. In fact, this method can be based on short samples, on expert assessments, individual measurements, which is what justifies its use for detecting random radio monitoring signals. An algorithm for detection and recognition of signals of means of covertly obtaining information based on the verification of statistical hypotheses is proposed. Mathematical modeling of two cases where the first a priori distribution of the signal parameter is uniform and the second case when the a priori distribution of the parameter is a normal distribution is carried out. Mathematical calculations showed the possibility of using Bayes' theorem to build an algorithm for detecting and recognizing signals of means of tacitly obtaining information. It is proved that if the sample mean has a normal distribution and a known variance, and the probability has a normal distribution, then the posterior distribution for the probability is also normal. The calculations proved the advantages of the second case for which the variance of the posterior distribution decreased from the value of 2.0 to 0.25, which led to a significant reduction in the uncertainty of this distribution due to the data obtained after radio monitoring. This proved the possibility of using Bayes' theorem to detect and recognize signals of means of tacitly obtaining information and the adequacy of the proposed algorithm.*

Keywords: *Bayes theorem, personal data, personal information, hypothesis, random signal, method, false information, clustering.*

1. Вступ.

Захист інформації став життєво-важливим аспектом нашого повсякденного життя. Зберігаючи інформацію у різноманітній формі та передаючи за допомогою різних технологій та пристроїв, є потреба в забезпеченні її цілісності та конфіденційності. Актуальність інформаційної безпеки у сучасному світі важлива з кількох причин. По-перше, з поширенням технологій і цифровизацією всіх сфер життя, дані стали однією з найцінніших активів. По-друге, кіберзагрози, такі як хакерські атаки, фішинг, віруси, поширюються і стають все більш складними. По-третє, після введення загального регламенту щодо захисту персональних даних та інших правових норм, організації змушені приділяти більше уваги захисту даних. На сучасний момент отримання конфедіційної інформації частиш за все здійснюються за допомогою засобів негласного отримання інформації. Це обумовлено наступними факторами, по перше після встановлення засобів негласного отримання інформації у приміщенні необхідність присутності фахівця відпадає. Знайти технічного розвідника дуже складно. Якщо припустити фактор використання при встановленні засобів негласного отримання інформації співробітників підприємства, або запрошених на нараду фахівців то варіант затримки розвідника практично виключено. По друге засоби негласного отримання інформації мають можливість отримати інформацію не перебуваючи безпосереднє в середині приміщень.

Ідентифікація загроз полягає в виявленні потенційних небезпек для безпеки інформації та оцінці їхнього впливу на активи організації. Це важливий етап у процесі оцінки ризиків інформаційної безпеки. З цією метою методи оцінки ризиків широко використовуються у системах математичного моделювання, зокрема у моделях ймовірнісного типу. Використання байєсівського аналізу даних разом з нечіткою логікою дозволяє враховувати невизначеності,

що виникають як у ймовірнісних, так і у амплітудних характеристиках, що забезпечує покращення якості ухвалених рішень. Таким чином, застосування методів байєсівського аналізу даних для підвищення ефективності захисту інформації є важливою науковою проблемою, яка дозволить ефективно виявляти загрози у системах захисту інформації.

2. Аналіз останніх досліджень і публікацій.

Багато публікацій присвячено питанням захисту інформації та розробці методів виявлення сигналів засобів нелегального отримання інформації. Для успішного виконання сучасних досліджень необхідно використовувати різноманітні методи. У роботі [1] детально розглядаються методи байєсівського аналізу даних, як і більшість методів ймовірнісно-статистичної обробки даних, що можуть ефективно адаптуватися до нових даних з метою підвищення адекватності будуються моделей. Підкреслюється, що ідея байєсівського аналізу даних базується на теоремі Байєса і передбачає повторне використання його при з'яві нових даних, фактів та експертних оцінок. Однак застосування теореми Байєса для виявлення випадкових радіосигналів є складною задачею.

У роботі [2] підкреслюється, що байєсівські методи можуть бути успішно застосовані для рішення широкого спектру завдань. Зокрема, вони особливо корисні у сфері менеджменту ризиків, оскільки ризик визначається як можливі втрати та їх ймовірність. Для ефективного розв'язання таких задач потрібно аналізувати розподіли та умовні ймовірності відповідних подій, пов'язаних з впливом факторів ризику на можливі результати реалізації ризиків. Проте робота не розглядає можливі варіанти підвищення ефективності захисту інформації в загальному контексті.

У роботах [4,5, 9-11] визначено ймовірнісні характеристики когерентного виявлення відбитих сигналів із повністю відомими параметрами при використанні стохастичних зондувальних радіосигналів. Наведені аналітичні співвідношення для щільності ймовірності вирішальної статистики за наявності лише відбитого сигналу на вході детектора, лише завади та за наявності як сигналу, так і завади. Розраховано залежності ймовірності помилкової тривоги від порогового відношення та ймовірності правильного виявлення відношення сигнал/шум при різних значеннях бази стохастичного сигналу, сімейство характеристик виявлення для фіксованої бази та різних значень розраховується ймовірність помилкової тривоги. Однак виявлення на основі прямих параметрів радіосигналів не розглядається.

У роботах [6-8] пропонується альтернативна концепція енергетичної теорії виявлення випадкових сигналів, розроблена на основі закону байєсівської безумовної оптимізації статистичних рішень. Процес виявлення випадкових сигналів визначається як пошук інтервалу часу, протягом якого загальна енергія сигналу та шуму, відносно середньої енергії внутрішнього шуму, перевищує встановлений поріг виявлення з визначеними якісними характеристиками. Досліджено методи послідовного та паралельного енергетичного виявлення радіосигналів на радіочастоті, енергія яких порівнюється з рівнем внутрішнього шуму радіоприймача, як без урахування, так і з урахуванням впливу зовнішніх активних маскувальних перешкод.

У роботах [12-17] наведено методи детектування каналів витоку інформації та їх узагальнення. Вхід до бази даних з послідовними методами аналізу. Проте питання аналізу інформації з метою розділення реальних і складних варіантів витоку інформації не піднімається. У результаті використовуються значні математичні та технічні ресурси. Що збільшує час на виявлення та блокування випадкових сигналів. Питання визначення ймовірності виявлення випадкових сигналів в літературі практично не розглядається.

Виходячи з вищевикладеного, дуже важливим є питання виявлення випадкових радіосигналів. А саме вирішення питання чи є випадковий сигнал, сигналом засобу негласного отримання інформації чи ні. Саме засоби негласного отримання інформації порушують конфедіційність інформації. Тому наукове завдання по розробці нових та удосконалення існуючих методів виявлення та блокування випадкових сигналів, сигналів якими є сигнали засобів негласного отримання інформації є дуже актуальним.

3. Мета і задачі дослідження.

Метою даної роботи є використання теореми Байєса для виявлення небезпеки у системі захисту інформації, а саме виявляти та розпізнавати сигнали засобів негласного отримання інформації, що дозволить підвищити ефективність захисту інформації загалом.

4. Результати дослідження.

Виявлення та розпізнавання випадкових радіосигналів є завданням перевірки статистичних гіпотез. В окремому випадку адитивних гаусівських шумів і деяких припущень завдання зводиться до синтезу фільтра, оптимального за критерієм максимального відношення сигнал/шум. Для розгляду цього питання наведемо основні відомості, що дозволяють вирішити задачу для спостереження сигналів у дискретному часі.

Нехай в результаті спостереження отримано вектор x, що представляє собою значення векторної випадкової величини X, що приймає значення з простору спостереження (діапазону радіомоніторінгу) Ωx. Приймаємо до увазі, що сигнали діапазону радіомоніторінга, які можуть бути адитивною сумішшю, мультиплікативну сумішшю або комбіновану суміш, тобто одним із заданого набору повністю відомих сигналів, які задано виразом $S_i = [S_i, S_{2i}, ..., S_{ni}]^T, i \in [0, m-1]$ і шуму (перешкоди) із заданою щільністю розподілу ймовірності.

Тоді завдання виявлення шкідливого сигналу є окремим випадком розпізнавання, коли m = 2, а один із сигналів тотожно дорівнює нулю: $S_0 = 0$.

Наприклад, при розпізнаванні двох сигналів S_0 та S_1 на тлі комбінованого адитивного V і мультиплікативного U шуму по спостереженню x слід проводити перевірку гіпотез:

$$H_o : X = U_S^0 + V, \quad H_1 : X = U_S^1 + V, \tag{1}$$

де $U = diag[U_1, U_2, ..., U_n]$ - випадкова матриця відліків мультиплікативних шумів;

$V = [V_1, V_2, ..., V_n]^T$ – випадковий вектор відліків адитивних шумів.

Завдання (1) можна подати у параметричному вигляді. Нехай випадкова величина ϑ може приймати значення з множини $\Omega_\vartheta = \{0;1\}$. Спостереження доступна реалізація буде випадкова величина:

$$X = (1-\vartheta)(U_{S0} + V) + \vartheta(U_{S1} + V) = (1-\vartheta)U_{S0} + \vartheta U_{S1} + V. \tag{2}$$

Потрібно перевірити гіпотези:

$$H_o : \vartheta = 0, \quad \vartheta = 1. \tag{3}$$

Наведений приклад показує, що за даної постановки завдання виявлення (розпізнавання) ймовірної величини (сигналу) X залежить від деякої випадкової величини $\vartheta \in \Omega_\vartheta$ (залежить від стану природи), значення якої ϑ у конкретному досвіді необхідно визначити.

Зауважимо, що при такому формулюванні завдання виявлення та оцінки параметрів сигналів нічим принципово ні різняться і вирішуються однаково.

Вважатимемо, що умовна функція розподілу $F_{X|\vartheta}(x|\theta) = P\{X < x | \vartheta = \theta\}$ (умовна щільність розподілу ймовірності) $W_{X|\vartheta}(x|\theta)$ та щільність розподілу ймовірності $W_\vartheta(\theta)$, відомі на початок дослідження.

Для наведеного прикладу простір дій A складається з двох елементів: a_0 і a_1, які відповідно означають прийняття гіпотези $H_0(\hat{\theta} = 0)$ *та* $H_1(\hat{\theta} = 1)$.

Простір рішень D складається з усіх відображень d: Ωx → A вектору спостережень у доступні дії. Таким чином, простір спостережень (радіомоніторінгу) поділяється на дві області: Ωx = {x | d(x) = a_o} прийняття гіпотези H_0 (вчинення дії a_o) та область Ωx = {x | d(x) =

$a_1\}$ прийняття гіпотези H_1 (вчинення дії a_1). Завдання синтезу оптимального виявлення сигналу полягає у проведенні цього розбиття. Зауважимо, що області Ω^I та Ω^{II} можуть бути незв'язними.

При даній постановці завдання кожній дії взаємно однозначно ставитися оцінка $\hat{\theta}$ стану (параметра) θ природи, тому простору A та Ωө можливо ототожнити: A = Ωө. Кожна дія (рішення про значення θ випадкового параметра Ωө у конкретному досвіді) супроводжується втратами, які описують функцією втрат $L:\Omega_\theta \times A \to R^+, \partial e \quad R^+$ — множина дійсних позитивних чисел. Функція втрат кожному істинному значенню θ стану (параметра) природи Ωө зіставляє оцінку $\hat{\theta} = \hat{\Omega}$ цього параметра. Оскільки рішення може супроводжуватися помилками, то у разі помилки особа, яка приймає рішення, зазнає збитків, які описуються функцією втрат. Зрозуміло, що функція втрат є невід'ємною функцією. При цьому втрати при правильному рішенні мають бути більше втрат при помилковому рішенні:

$$L = (\theta, \hat{\theta}) > L(\theta, \theta) \text{ якщо } \theta \neq \hat{\theta},\ A = \Omega_\theta,\ d(x) = \hat{\theta}. \tag{4}$$

Кожному рішенню d = d(x) та стану природи θ зіставимо ризик

$$R(\theta, d) = \int_{\Omega x} L(\theta, d(x)) W_{X|\theta}(x \mid \theta) dx = E\{L(\theta, d(X)) | \theta = 0\}. \tag{5}$$

Критерій оцінки Байєса.

Байєсівська перевірка гіпотез - це статистичний метод, який дозволяє дослідникам оцінити докази на користь і проти конкуруючих гіпотез, виходячи з ймовірності спостережуваних даних за кожною гіпотезою, а також попередньої ймовірності кожної гіпотези. На відміну від класичної перевірки гіпотез, яка зосереджена на відкиданні нульових гіпотез на основі p-значень, байєсівська перевірка гіпотез забезпечує більш тонкий та інформативний підхід до перевірки гіпотез, дозволяючи дослідникам кількісно оцінити силу доказів на користь і проти кожної гіпотези.

При байєсівській перевірці гіпотез дослідники починають з попереднього розподілу ймовірностей для кожної гіпотези, що базується на наявних знаннях або переконаннях. Потім вони оновлюють попередній розподіл ймовірностей на основі ймовірності спостережуваних даних для кожної гіпотези, використовуючи теорему Байєса. Отриманий в результаті апостеріорний розподіл ймовірностей представляє ймовірність кожної гіпотези, враховуючи спостережувані дані.

Сила доказів на користь однієї гіпотези порівняно з іншою може бути кількісно оцінена шляхом обчислення коефіцієнта Байєса, який є відношенням ймовірності спостережуваних даних за однією гіпотезою до іншої, зваженої на їхні попередні ймовірності. Фактор Байєса, більший за 1, свідчить на користь однієї гіпотези, тоді як фактор Байєса, менший за 1, свідчить на користь іншої гіпотези.

Байєсовське вирішальне правило $d^* = d^*(x) \in A$ обирають з умови мінімуму середнього ризику:

$$r(d^*) = \min_{d \in D} \int_{\Omega\theta} R(\theta, d(x)) W_\theta(\theta)\, d\theta. \tag{6}$$

Можливо визначити, що байєсовська вирішальна функція може бути знайдена з умови мінімуму апостеріорного ризику.

Характеристики виявника. Для задачі (3) (за умови A = Ωө = {0;1}) головними характеристиками виявника є:

а) ймовірність хибної тривоги α = P {d(X) = 1 | ө = 0}, що дорівнює ймовірності прийняти гіпотезу H_1 про наявність корисного сигналу в той час, як корисний сигнал відсутній;

б) можливість пропуску сигналу β = P{d(X) = 0 | ө = 1}, що дорівнює ймовірності прийняти гіпотезу H_0 про відсутність корисного сигналу в той час як корисний сигнал

присутній;

в) ймовірність правильного виявлення Qd = P {d(X) = 1 | ɵ = 1} = 1-β, дорівнює ймовірності прийняти гіпотезу H_1 про наявність корисного сигналу в той час, як корисний сигнал справді присутній;

г) ймовірність повної помилки Qd = αP { ɵ = 0} + βP { ɵ = 1}.

Величину α називають рівнем значущості критерію d(x), а величину Qd - потужністю критерію.

Байєсівська перевірка гіпотез має кілька переваг над класичною перевіркою гіпотез. По-перше, вона дозволяє дослідникам оновити свої попередні переконання на основі спостережуваних даних, що може призвести до більш точних і надійних висновків. По-друге, воно забезпечує більш інформативну міру доказів, ніж імовірні значення, які лише вказують, чи є спостережувані дані статистично значущими на заздалегідь визначеному рівні. Нарешті, він може враховувати складні моделі з багатьма параметрами і гіпотезами, які може бути важко проаналізувати за допомогою класичних методів.

Загалом, байєсівська перевірка гіпотез є потужним і гнучким статистичним методом, який може допомогти дослідникам приймати більш обґрунтовані рішення і робити більш точні висновки на основі своїх даних.

Випадок нормально розподілених даних з відомою дисперсією і невідомим середнім.

Наведемо приклад застосування запропонованого методу у декілька випадків, для виявлення випадкових сигналів, які можуть бути сигналами засобів негласного отримання інформації

У випадку обмеженої апріорної інформації, перший сценарій передбачає рівномірний розподіл параметру сигналу. Тут параметр сигналу відноситься до факторів виявлення сигналів, таких як амплітуда, спектр, потужність та інші. Ми припускаємо, що немає чіткої інформації щодо ефективності виявлення радіосигналів, що можуть бути сигналами засобів негласного отримання інформації. У зв'язку з цим, значення параметру θ можуть знаходитись у широкому діапазоні дійсних чисел з однаковою ймовірністю, тому вибирається рівномірний розподіл для можливих значень θ. Рівномірний розподіл, який описується неналежною апріорною щільністю, фактично передбачає константне значення на всьому діапазоні визначення даного параметра. Такий вибір апріорної щільності розподілу можна формально виразити як: $g(\theta) \propto c = стала\ величина$, для всіх θ : $-\infty < \theta < +\infty$. Виходячи з цього такий вибір можливо записати у вигляді:

$$g(\theta) = \lim_{a \to \infty} \left(\frac{1}{2a} \right), \quad -a < \theta < a. \tag{7}$$

Будемо застосовувати до статистичних даних, статистичні дані це параметри, які ми обрали та які виявили у результати моніторингу обраного радіодіапазону, теорему Байєса у вигляді наведеним виразом (8):

$$h(\theta | x_1, x_2, ..., x_n) \propto L(x_1, x_2, ..., x_n | \theta)\, g(\theta), \tag{8}$$

де L(·) – функція правдоподібності для даних; g(θ) – апріорна щільність розподілу ймовірностей для параметра θ ; $h(\theta | x_1, x_2, ..., x_n)$ – апостеріорна щільність розподілу ймовірностей для цього параметра.

Також необхідно підкреслити, що $h(\theta | x_1, x_2, ..., x_n)$ залежить від даних тільки через функцію правдоподібності для L(x) для даних. Інтеграл у знаменнику береться по всіх значеннях θ і не повинен дорівнювати нулю. Дані можуть бути багатовимірними і корельованими, а θ може бути вектором параметрів.

Спростимо теорему Байеса записану виразом (7), за рахунок підстановки обраного плоского розподілу для θ, отримаємо вираз (7) у вигляді:

$$h(\theta \mid x_1, x_2, ..., x_n) \infty L(x_1, x_2, ..., x_n \mid \theta). \quad (9)$$

Давайте складемо функцію правдоподібності, використовуючи вибіркове середнє для n = 100. Щоб обчислити дисперсію для цієї групи, кожне індивідуальне значення потрібно розділити на 100, оскільки ми маємо 100 значень параметрів сигналів для цієї групи (x|θ) ~ N (θ, 25/ n) = N (θ; 0,25), то апостеріорна щільність буде приймати вигляд, який визначається виразом (10):

$$h(\theta \mid \bar{x}) \infty \exp\left\{(-0,25)\left(\frac{\bar{x}-\theta}{0,25}\right)^2\right\}. \quad (10)$$

Апостеріорна щільність для параметра θ буде мати такий розподіл: (θ| x) ~ N (x; 0,25). Зауважимо, що незважаючи на те, що апріорний розподіл був обраний як неналежний, апостеріорний розподіл став належним і має нормальний характер. Додатково, оскільки апріорна інформація була дуже обмеженою, головну роль відіграв експеримент, і апостеріорний розподіл концентрується навколо вибіркового середнього. Оскільки ця оцінка відповідає методу максимальної правдоподібності, ми отримали кращий варіант серед можливих. Дисперсія апостеріорного розподілу зменшилась до 0,25 через великий обсяг вибірки (n = 100). Цей приклад ілюструє перевагу використання пропорційної форми теореми Байєса. Не було необхідності виконувати формальне інтегрування у знаменнику, оскільки форму сімейства апостеріорного розподілу можна було визначити на основі ядра апостеріорного розподілу.

Якщо зробити припущеня, що вибіркове середнє $\bar{x} = 3$; то апостеріорний розподіл буде приймати вигляд: (θ| x) ~ N (3; 0,25). Зробивши аналізу апостеріорного розподілу, довели, що в результаті радіомоніторингу заданого радіодіапазону середнє значення скорингу (у нашому випадку оцінка ризику помилки невизначення сигналів негласного отримання інформації) знаходиться в інтервалі (1,15; 5,35) з ймовірністю 0,998. Це доводить то, що у цьому інтервалі отримана крива розподілу охоплює 99,7% площі розподілу.

Другій випадок. Наступне припущення - апріорний розподіл параметра пвдпорядковується нормальному закону.

Друге припущеня, перший варіант моніторингу зміни (прирости) середнього скорингу параметру θ для параметрів сигналів мали розподіл (θ) ~ N (5; 2,0). Будемо приймати цей розподіл за апріорний. В загалі, у більш відомій формі апріорний розподіл має такий вигляд: $(\theta) \sim N(m, \sigma^2)$, або у іншому вигляді:

$$g(\theta \mid \bar{x}) \infty \exp\left\{(-0,25)\left(\frac{\theta-m}{\sigma}\right)^2\right\}. \quad (11)$$

Зробимо підстановку цього виразу в вираз (7) отримаємо:

$$h(\theta \mid \bar{x}) \infty \exp\left\{(-0,25)[\left(\frac{\theta-m}{\sigma}\right)^2 + \left(\frac{\bar{x}-\theta}{0,25}\right)^2]\right\}, \quad (12)$$

де $\exp\left\{(-0,25)\left(\frac{\bar{x}-\theta}{0,25}\right)^2\right\}$ взято з попереднього випадку.

Після спрощення будемо мати вираз:

$$h(\theta \mid \bar{x}) \infty \exp\left\{(-0,25)\left(\frac{\theta-\bar{\theta}}{\gamma}\right)^2\right\}, \quad (13)$$

де $\frac{1}{\gamma^2} = \frac{1}{\sigma^2} + \frac{1}{(0,25)^2}$, а оцінка середнього значення для параметра θ :

$$\overline{\theta} = m\left(\frac{\sigma^{-2}}{\sigma^{-2}+(0{,}25)^{-2}}\right)+\overline{x}\left(\frac{(0{,}25)^{-2}}{\sigma^{-2}+(0{,}25)^{-2}}\right). \quad (14)$$

Тобто, $(\theta \mid \overline{x}) \approx N(\overline{\theta}, \gamma^2)$. Доведено, що, у випадку, коли вибіркове середнє $\overline{x}$ має нормальний розподіл із середнім параметром θ і відомою дисперсією, тоді апостеріорний розподіл для параметра θ буде також нормальний.

У випалку коли прийняти за точність оцінювання (розподілу) величину обернену дисперсії, тоді апостеріорна точність γ^{-2} дорівнює сумі точності апріорного розподілу σ^{-2} і точності вибіркового (експериментального) розподілу $(0{,}5)^{-2}$. Апостеріорне середнє параметра $\overline{\theta}$ – це опукла комбінація зваженого апріорного середнього m і вибіркового середнього $\overline{x}$. Вагові коефіцієнти пропорційні точності (оцінювання), яка відповідає апріорному та вибірковому розподілам. Відповідно до виконаних розрахунків, отримано такі параметри апостеріорного розподілу, які визначаються :

$$\overline{\theta} \approx N(3{,}37; 0{,}25).$$

Таким чином, найбільш ймовірне значення параметру середнього θ, зменьшилось та змістилось від значення 5,0 до 3,37. Також, дисперсія апостеріорного розподілу зменшилась із значення 2,0 до значення 0,25. Це привело до значного зменшення невизначеності цього розподілу, саме завдяки отриманим даних після радіомоніторингу.

5. Висновки.

Таким чином запропоновано алгоритм виявлення та розпізнавання сигналів засобів негласного отримання інформації на основі перевірки статистичних гіпотез. Проведено математичне моделювання двох випадків перший апріорний розподіл параметру сигналу рівномірний та другій випадок коли апріорний розподіл параметра нормальний розподілу. Математичні розрахунки показали можливість використання теореми Байєса для побудови алгоритму виявлення та розпізнавання сигналів засобів негласного отримання інформації. Доведено, що у випадку, коли вибіркове середнє має нормальний розподіл і відомою дисперсією, а імовірність має нормальний розподіл, то апостеріорний розподіл для імовірності також нормальний. Розрахунки довели переваги другого випадку для якого дисперсія апостеріорного розподілу зменшилась із значення 2,0 до значення 0,25, що привело до значного зменшення невизначеності цього розподілу завдяки отриманим даних після радіомоніторингу. Це довело можливість використання теореми Байєса для виявлення та розпізнавання сигналів засобів негласного отримання інформації та адекватність запропонованого алгоритму.

Аналіз наукової літератури та проведене дослідження показало, що тільки комплексний підхід до захисту інформації, а саме заходи з підвищення ефективності інформаційної безпеки, які повинні включати інженерно-технічні, організаційно-правові та апаратно-програмні заходи можуть забезпечити повноцінний захист інформації в організації. Тому напрямком подальших досліджень може бути удосконалення інших напрямків захисту інформації, а саме апаратно-програмних методів захисту інформації.

Список використаної літератури

1. Zamrii I., Sobchuk V., Laptiev O., Savchenko V., Shkapa V., Kovalenko V. and Kotok V. Fractal Functions and Their Application to Source Data Coding. ARPN Journal of Engineering and Applied Sciences. Vol. 17, No. 4, 2022. pp. 424 – 435.

2. Тетяна Лаптєва. Алгоритм визначення міри існування недостовірної інформації в

умовах інформаційного протиборства. Кібербезпека: освіта, наука, техніка. No 2 (14), 2021, с. 15-25.

3. Наконечний В. С., Барабаш О. В., Лаптєва Т. О., Міщенко А. В. Удосконалення методу виявлення та кластерізації джерел неправдивої інформації. Наукоємні технології. Інформаційні технології, кібербезпека. Том 54 № 4 (2022) стр.105 - 111. DOI 10.18372/2310-5461.54.16747

4. Жигалкевич Ж.М. Кластери взаємодіючих підприємств та їх класифікація .Вісник ОНУ імені І.І. Мечникова , 2014. Т. 19, Вип. 2/3. с. 98-101.

5. Лаптєва Т.О., Лукова-Чуйко Н.В., Собчук А.В. Дослідження основних загроз і оцінка безпеки інформаційних систем. Математика. Інформаційні технології. Освіта. 2022 рік: збірка тез допов. учасник. XI Міжнар. наук.–практ. конф., 3–5 червня 2022 р. Луцьк–Світязь: СНУ імені Лесі Українки, 2022. с. 101-103

6. Рябий М. О. Хатян О. А., Багацький С. П. Модель виявлення PR-впливу через публікації в інтернет ЗМІ. Інформаційна безпека. 2015. Т. 21, № 2. с. 131-1.39.

7. Поліщук Ю. Я., Гнатюк С. О., Сейлона П. А. Мас медіа як канал маніпулятивного впливу на суспільство. Інформаційна безпека. 2015. Т. 21, Ч. 3. с. 301-308.

8. V. Theocharis, W. Lowe, J. W. van Deth, G. Garcla-Albacete .Using Twitter to mobilize protest action: Online mobilization patterns and action repertoires in the Occupy Wall Street, Indignados, and Aganaktismenoi movements. Information, Communication & Society . 2015. 18. pp. 202-220.

9. Butko, T., Prokhorchenko, A., Muzykin, M. An improved method of determining the schemes of locomotive circulation with regard to the technological peculiarities of railcar traffic. Eastern-European Journal of Enterprise Technologies. 2016. 5(3 (83)), pp. 47–55.

10. Молодецька К. В. Підхід до виявлення організаційних ознак інформаційних операцій у соціальних інтернет-сервісах. Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв'язку та автоматизації в АТО : збірн. матер. IX наук.-практ. конф., 25 листоп. 2016 р. Київ: ВІТІ. 2016. С. 130-131.

11. Faraz A. A comparison of text Categorization methods . International Journal on Natural Language Computing. 2016.-5(1). pp. 31 -44.

12. Лаптєв О.А., Бабенко Р.В., Правдивий А.М., Зозуля С.А., Стефурак О.Р. Удосконалена методика вибору послідовності пріоритетів обслуговання потоків інформації. Науково-практичний журнал «Зв'язок». К. : ДУТ, 2020. №4 (146), С.27 – 31.

13. O.Svynchuk, O. Barabash, J.Nikodem, R. Kochan, O. Laptiev. Image compression using fractal functions.Fractal and Fractional, 2021, 5(2), 31.pp.1-14.

14. Zamrii I., Sobchuk V., Laptiev O., Savchenko V., Shkapa V., Kovalenko V. and Kotok V. Fractal Functions and Their Application to Source Data Coding. ARPN Journal of Engineering and Applied Sciences. Vol. 17, No. 4, 2022. pp. 424 – 435

15. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov and others/ Synergy of building cybersecurity systems. Kharkiv. Publisher PC TECHNOLOGY CENTER. 2021 – 188 c.

13. Лукова-Чуйко Н., Герасименко О., Толюпа С., ...Лаптієва Т., Лаптієв О. Спосіб детектування радіосигналів шляхом оцінки параметрів сигналів поворотного гауссового поширення. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 - Матеріали, 2021, стор. 67–70.

14. Власик Г., Замрій І., Шкапа В., ... Калинюк А., Лаптєв А Т. Спосіб вирішення задач оптимального відновлення телекомунікаційних сигналів. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 - Матеріали, 2021, стор. 71–75.

15. Бідюк П.І. Байєсівський аналіз даних : монографія / П.І. Бідюк, І.О. Калініна, О.П. Гожий. – Херсон: Книж. вид-во ФОП Вишемирський В.С., 2021. – 208 с.

16. Serhii Laptiev. Удосконалений метод захисту персональних даних від атак за

допомогою алгоритмів соціальної інженерії. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка, 4(16), 2022. С. 45–62.

17. S. Laptiev, S. Tolupa. The methodology for evaluating the functional stability of the protection system of special networks. Наукоємні технології. Інформаційні технології, кібербезпека. Том 55 № 3 (2022) С.178 – 183.

References

1. Zamrii I., Sobchuk V., Laptiev O., Savchenko V., Shkapa V., Kovalenko V. and Kotok V. Fractal Functions and Their Application to Source Data Coding. ARPN Journal of Engineering and Applied Sciences. Vol. 17, No. 4, 2022. pp. 424-435.

2. Tetiana Laptieva. Algorithm for determining the degree of existence of unreliable information in the conditions of information conflict. Cyber security: education, science, technology. No. 2 (14), 2021, p. 15-25.

3. V. S. Nakonechnyi, O. V. Barabash, T. O. Laptieva, and A. V. Mishchenko. Improvement of the method of detection and clustering of sources of false information. Scientific technologies. Information technologies, cyber security. Volume 54 No. 4 (2022) pp. 105 - 111.

4. Zhigalkevich Zh.M. Clusters of interacting enterprises and their classification. Bulletin of ONU named after I.I. Mechnikova, 2014. T. 19, Issue 2/3. with. 98-101.

5. Lapteva T.O., Lukova-Chuiko N.V., Sobchuk A.V. Study of the main threats and assessment of the security of information systems. Math. Information Technology. Education. 2022: a collection of theses add. member. XI International science and practice conference, June 3–5, 2022. Lutsk–Svityaz: Lesya Ukrainka SNU, 2022. p. 101-103

6. Ryabiy M. O. Khatyan O. A., Bagatskyi C. P. A model for detecting PR influence through publications on the Internet mass media. Informational security. 2015. Vol. 21, No. 2. p. 131-1.39.

7. Polishchuk Y. Ya., Hnatiuk S. O., Seilona P. A. Mac media as a channel of manipulative influence on society. Informational security. 2015. Vol. 21, Part 3. p. 301-308.

8. V. Theocharis, W. Lowe, J. W. van Deth, G. Garcla-Albacete. Using Twitter to mobilize protest action: Online mobilization patterns and action repertoires in the Occupy Wall Street, Indignados, and Aganaktismenoi movements. Information, Communication & Society. 2015. 18. pp. 202-220.

9. Butko, T., Prokhorchenko, A., Muzykin, M. An improved method of determining the schemes of locomotive circulation with regard to the technological peculiarities of railcar traffic. Eastern-European Journal of Enterprise Technologies. 2016. 5(3 (83)), pp. 47–55.

10. Molodetska K. V. Approach to identifying organizational features of information operations in social Internet services. Priority areas of development of telecommunication systems and special purpose networks. Application of divisions, complexes, means of communication and automation in ATO: collection. the mother IX science-practice conference, November 25 2016. Kyiv: VITI. 2016. P. 130-131.

11. Faraz A. A comparison of text categorization methods. International Journal on Natural Language Computing. 2016.-5(1). years 31-44.

12. Laptev O.A., Babenko R.V., Pravdyviy A.M., Zozulya S.A., Stefurak O.R. An improved technique for choosing the sequence of priorities for servicing information flows. Scientific and practical magazine "Zvyazok". K.: DUT, 2020. No. 4 (146), pp. 27-31.

13. O. Svynchuk, O. Barabash, J. Nikodem, R. Kochan, O. Laptiev. Image compression using fractal functions. Fractal and Fractional, 2021, 5(2), 31.pp.1-14. DOI:10.3390/fractalfract5020031 - 14 Apr 2021

14. Zamrii I., Sobchuk V., Laptiev O., Savchenko V., Shkapa V., Kovalenko V. and Kotok V. Fractal Functions and Their Application to Source Data Coding. ARPN Journal of Engineering and Applied Sciences. Vol. 17, No. 4, 2022. pp. 424-435

15. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov and others/ Synergy of building cybersecurity systems. Kharkiv. Publisher PC TECHNOLOGY CENTER. 2021 – 188 p.

13. Lukova-Chuiko N., Gerasimenko O., Tolyupa S., ...Laptieva T., Laptiyev O. The method of detecting radio signals by estimating the parameters of signals of rotary Gaussian propagation. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 - Proceedings, 2021, p. 67–70.

14. Vlasyk H., Zamriy I., Shkapa V., ... Kalynyuk A., Lapteva T. A method of solving problems of optimal restoration of telecommunication signals. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 - Proceedings, 2021, p. 71–75.

15. Bidyuk P.I. Bayesian data analysis: monograph / P.I. Bidyuk, I.O. Kalinina, O.P. Gozhiy – Kherson: Book. Vyshemyrsky V.S., 2021. – 208 p.

16. Serhii Laptiev. An improved method of protecting personal data from attacks using social engineering algorithms. Electronic specialized scientific publication "Cybersecurity: education, science, technology", 4(16), 2022. P. 45–62.

17. S. Laptiev, S. Tolupa. The methodology for evaluating the functional stability of the protection system of special networks. Scientific technologies. Information technologies, cyber security. Volume 55 No. 3 (2022) C.178 – 183.