ternational Conference on Software Engineering Workshops, June 2020, pp. 545-548. doi: 10.1145/3387940.3392265.
[24]. Cannavacciuolo, C., Mariani, L., "Smoke Testing of Cloud Systems," 2022 IEEE Conference on Software Testing, Verification and Validation (ICST), Valencia, Spain, 2022, pp. 47-57. doi: 10.1109 / ICST53961.2022.00016.
[25]. Chen, Q. Z., Schnabel, T., Nushi, B., & Amershi, S. HINT: Integration Testing for AI-based features with Humans in the Loop. IUI '22 Proceedings of the 27th International Conference on Intelligent User Interfaces, March 2022, pp. 549-565. doi: 10.1145/3490099.3511141.
[26]. Yoo, S., & Harman, M. Regression testing minimization, selection and prioritization: a survey. John Wiley & Sons, Ltd., 2012/3, Vol.22, Issue 2, pp. 67-120. doi: 10.1002/stvr.430.
[27]. Liu, Y., Li, Y., Deng, G., Liu, Y., Wan, R., Wu, R., Ji, D., Xu, S., & Bao, M. Morest: Model-based RESTful API Testing with Execution Feedback. arXiv:2204.12148, 2022. doi: 10.48550/arXiv.2204.12148.
[28]. Qasaimeh M, Hammour RA, Yassein MB, Al-Qassas RS, Torralbo JAL, Lizcano D. Advanced security testing using a cyber-attack forecasting model: A case study of financial institutions. J Softw Evol Proc. 2022; 34(11): e2489. doi: 10.1002/smr.2489.
[29]. Chen, S., Haque, M., Liu, C., & Yang, W. DeepPerform: An Efficient Approach for Performance Testing of Resource-Constrained Neural Networks. ASE '22 Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering, October 2022, Article No.:31, pp. 1-13. doi: 10.1145/3551349.3561158.
[30]. Wickström, O., & O'Connor, L. Quickstrom: property-based acceptance testing with LTL specifications. PLDI 2022 Proceedings of the 43rd ACM SIGPLAN International Conference on Programming Language Design and Implementation, June 2022, pp. 1025-1038. doi: 10.1145/3519939.3523728.
[31]. Abdillah, E. J., Khoriyah, R., Abqariy, A. N., & Susilo, P. H. (2022). Pengembangan Keamanan Website Menggunakan Teknik Penetration Testing dan DAST (Dynamic Application Security Testing). Media Jurnal Informatika, Vol 14, No 2 (2022), ISSN: 2477-2542. doi: 10.35194/mji.v14i2.2546.

DEVELOPMENT OF EFFECTIVE WEB SECURITY MEASURES FOR THE NETWORK BY CONDUCTING PENETRATION TESTING USING THE OWASP FRAMEWORK

With each step in the development of technology, web security is becoming a more relevant component for ensuring the reliability and protection of network systems. The growing number of cyber threats and potential security breaches emphasizes the need to improve the protection of network systems. To help developers and administrators in this process, there is an important tool – the OWASP (Open Web Application Security Project) framework. It provides a wide range of tools, guidelines, and resources for securing web applications. This framework helps developers check web applications for potential vulnerabilities and find ways to fix them. To better understand, you can imagine that the network is a house and web applications are its doors and windows. If these doors and windows are not tightly closed, attackers can easily get in and cause damage. So, to put it in comparison, just as you check if all the doors and windows in your network are secure, OWASP provides a means to check web applications for vulnerabilities that can be exploited by attackers. Therefore, using the OWASP framework is an important step in developing effective web security measures for your network, helping to ensure that your system is reliable and protected from possible cyberattacks and malicious actions.

Keywords: OWASP framework, web security, penetration testing, data protection, cyber security.

Піскозуб Андріян Збігнєвич, к.т.н., доцент, доцент кафедри Захисту інформації Національного університету «Львівська політехніка».

Piskozub Andrian, Ph.D., Associate Professor at the Department of Information Security, Lviv Polytechnic National University.
E-mail: andriian.z.piskozub@lpnu.ua.
Orcid ID: 0000-0002-3582-2835.

Козловська Марія Іванівна, студентка кафедри Захисту інформації Національного університету «Львівська політехніка».

Kozlovska Mariia, Student at the Department of Information Security, Lviv Polytechnic National University.
E-mail: mariia.kozlovska.kb.2021@lpnu.ua.
Orcid ID: 0009-0003-4959-0312.

DOI: 10.18372/2410-7840.26.18834
УДК 336.71:004.056

АЛГОРИТМ ЗАСТОСУВАННЯ ТЕОРЕМИ БАЙЄСА ДЛЯ ВИЯВЛЕННЯ НЕПРАВДИВОЇ ІНФОРМАЦІЇ У СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сергій Глухов, Ігор Половінкін, Максим Кузьменко, Віталій Пономаренко

Захист інформації стає більш актуальним у сучасному світі. Це пов'язано зі зростанням технічного прогресу та перетворенням світу у інформаційних світ. Особливо це стало помітним після всесвітнього карантину від короно вірусу, людство перейшло загалом у інформаційне спілкування. Набули подальший розвиток соціальні мережи та загалом інформаційне спілкування через всесвітню мережу інтернет- кіберпростір. В зв'язку з чим виникає наукове завдання по розробки нових та удосконаленню існуючих методів захисту інформації.

Одним з напрямків підвищення захисту інформації є застосування теореми Байєс. У роботі запропоновано практичне застосування теореми Байєса, що до підвищення ефективності виявлення небезпеки у системі захисту інформації та інформаційної безпеки Держави. Математичними розрахунками доведено доцільність використання теореми Байєса для виявлення порушення конфіденційності та правдивості інформації. За результатами розрахунків з використанням конкретних припущень отримали апостеріорне свідчення на користь того, що спектр сигналу є спектром сигналу засобу негласного отримання інформації складає біля 33:1, а для визначення неправдивої інформації апостеріорний шанс того, що інформація не є неправдивою інформацією 10:1, це є гарними результатами. Таким чином довели, що використання теореми Байєса для визначення захищеності інформації за запропонованим алгоритмом є удосконаленням методу оцінки захисту інформації та дозволяє вирішувати наукове завдання по підвищенню ефективності захисту інформації та інформаційної безпеки Держави.

***Ключові слова**: алгоритм, нелінійна система, стійкість, запізнення, прогнозування, інформаційні технології, неправдива інформація, персональні дані.*

ВСТУП

Захист інформації стає більш актуальним у сучасному світі. Це пов'язано зі зростанням технічного прогресу та перетворенням світу у інформаційних світ. Особливо це стало помітним після всесвітнього карантину від короно вірусу, людство перейшло загалом у інформаційне спілкування. Набули подальший розвиток соціальні мережи та загалом інформаційне спілкування через всесвітню мережу інтернет- кіберпростір. В зв'язку з чим виникає наукове завдання по розробки нових та удосконаленню існуючих методів захисту інформації. Одним з напрямків підвищення захисту інформації є застосування теореми Байєса для аналізу випадкових дій, які спрямовані на порушення конфіденційності та цілісності інформації. Теорема Байєса дозволяє описати ймовірність події, ґрунтуючись на минулому (апріорному) знанні умов, які можуть належати до подій. Ця теорема дозволяє враховувати суб'єктивну оцінку чи рівень довіри у суворих статистичних розрахунках. Це один із методів, який дозволяє поступово оновлювати ймовірність події в міру надходження нових спостережень чи відомостей. Суть роботи полягає у тому, що ми починаємо з гіпотези та рівня довіри до цієї гіпотези. Це означає, що на основі знання предметної галузі чи попередніх інших знань ми приписуємо цій гіпотезі ненульову ймовірність. Потім ми збираємо дані та оновлюємо наші первісні переконання.

Якщо нові дані підтверджують гіпотезу, то ймовірність зростає, а то й підтверджують - ймовірність знижується. Таким чином ми маємо можливість отримати позитивний вирок, що до гіпотез. У нашому випадку перший набір гіпотез, це існує сигнал засобів негласного отримання інформації або ні. Та у другому випадку інформація є правдивою чи недостовірною. Що дуже суттєво впливає на захист інформації у цілому.

Отримання конфіденційної інформації частіш за все робиться технічними засобами. Порушення інформаційної безпеки Держави здійснюється за допомогою розповсюдження неправдивої інформації. Тому розробка нових та удосконаленню існуючих методів захисту інформації є актуальним науковим завданням.

МЕТА РОБОТИ

Метою даної роботи є розробка алгоритму використання теореми Байєса для виявлення загроз у системах інформаційної безпеки, а саме виявляти та розпізнавати сигнали засобів негласного отримання інформації та виявляти і блокувати недостовірну інформацію, що дозволить підвищити ефективність захисту інформації загалом.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Успішне виконання сучасних досліджень вимагає застосування самих різноманітних методів, які можуть бути використані для розв'язання задач в умовах наявності невизначеностей, відсутності необхідних об'ємів даних стосовно розвитку досліджуваних процесів. Основною 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 окремих фактах, експертних оцінках, окремих вимірах, що є саме обґрунтовує використання його для виявлення випадкових сигналів радіомоніторингу.

Питанням захисту інформації, розробки методів виявлення сигналів засобів нелегального отримання інформації присвячено значну кількість публікацій. Так в роботі [1] розглядаються методи байєсівського аналізу даних, як і більшість методів ймовірнісно-статистичної обробки даних, які можуть бути успішно використані для

адаптування структури і параметрів моделей до нових даних з метою підвищення адекватності моделей, що будуються. Доводиться. що ідея байєсівського аналізу даних, що ґрунтується на використанні теореми Байєса, передбачає її повторне використання при появі нових вимірів, фактів та експертних оцінок. Однак узагальненого методу застосування теореми Байєса для виявлення неправдивої інформації та виявлення випадкових радіосигналів за різними параметрами не розглядається.

У роботі [2] коло задач, які можна розв'язувати байєсівськими методами. надзвичайно широке. В першу чергу це задачі менеджменту ризиків різної природи, оскільки за означенням ризику – це величина можливих втрат та їх ймовірність. Тобто при розв'язуванні таких задач необхідно оцінювати характеристики розподілів та умовні ймовірності відповідних подій, пов'язаних з аналізом впливу факторів ризику на можливі результати реалізації ризиків. Однак варіанти підвищення ефективності виявлення неправдивої інформації та радіосигналів засобів негласного отримання інформації не розглядається.

У роботах [4, 5, 9-11] визначено ймовірнісні характеристики когерентного виявлення відбитих сигналів із повністю відомими параметрами при використанні стохастичних зондувальних радіосигналів. Отримано аналітичне 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] запропоновано альтернативний варіант енергетичної теорії детектування неправдивої інформації, розроблений на основі закону байєсівської безумовної оптимізації статистичних рішень. Виявлення неправдивої інформації та виявлення випадкових сигналів – це пошук інтервалу часу, де сумарна енергія сигналу та шуму по відношенню до середньої енергії внутрішнього шуму перевищує поріг виявлення із заданими якісними показниками. Розглянуто методи послідовного та паралельного енергетичного детектування радіосигналів на радіочастоті від енергії, порівнянної або меншої за рівень внутрішнього шуму радіоприймача, без урахування та з урахуванням впливу зовнішніх активних маскувальних перешкод.

У роботах [12-16] наведено методи детектування неправдивої інформації та їх узагальнення. Вхід до бази даних з послідовними методами аналізу. Проте питання аналізу інформації з метою розділення реальних і складних варіантів застосування неправдивої інформації не піднімається. У результаті використовуються значні математичні та технічні ресурси. Що збільшує час на виявлення та блокування неправдивої інформації. Питання визначення ймовірності виявлення способу неправдивої інформації в літературі практично не розглядається.

Виходячи з вищевикладеного, дуже важливим є питання виявлення неправдивої інформації та виявлення випадкових радіосигналів. А саме вирішення питання чи є випадковий сигнал, сигналом засобу негласного отримання інформації чи ні. Є інформація правдивою чи ні. Саме засоби негласного отримання інформації порушують конфіденційність інформації, а неправдива інформація руйнує інформаційну безпеку Держави. Тому наукове завдання по розробці нових та удосконалення існуючих методів виявлення та блокування неправдивої інформації та виявлення випадкових сигналів, сигналів якими є сигнали засобів негласного отримання інформації є дуже актуальним.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У даній роботи розглянемо алгоритм та практичні аспекти застосування теореми Байєса до виявлення загроз у системах інформаційної безпеки. А саме запропонуємо алгоритм використання теореми Байєса для виявлення сигналів засобів негласного отримання інформації та виявлення неправдивої інформації з метою заборони її подальшого розповсюдження у інформаційному просторі.

Використання теореми Байєса для обробки та виявлення сигналів засобів негласного отримання інформації

Для пошуку сигналів засобів негласного отримання інформації існують багато методів ідентифікації, для нашого випадку будемо використовувати тільки декілька з них, тобто зробимо припущення, що саме ці ознаки виявлення є головними.

Але існує база спектрів сигналів, які є спектрами сигналів засобів негласного отримання інформації. Таким чином можливо виявляти випа-

дкові сигнали при радіомоніторингу та робити порівняння з існуючій базою спектрів сигналів засобів негласного отримання інформації

Наведемо приклад та зробимо розрахунки. Нехай після проведеного радіомоніторингу виявлено випадковий сигнал, який містять інформацію щодо сигналу засобів негласного отримання інформації (наприклад, перевищення амплітуди порога сканування, наявність другої та третій гармоніки і т. ін.). Припустимо, що цей сигнал дійсно є сигналом засобу негласного отримання інформації. Таким чином, спектр цього сигналу необхідно співставити з базою спектрів сигналів які є спектрами сигналів існуючої бази. Застосуємо для розв'язку цієї задачі теорему Байєса.

Введемо в розгляд такі події:

– C – випадковий спектр сигналу є спектром сигналу засобу негласного отримання інформації;

– $\bar{C}$ – випадковий спектр сигналу не є спектром сигналу засобу негласного отримання інформації;

– M – спектр сигналу, визначене радіомоніторингом, збігаються;

– $\bar{M}$ – спектр сигналу, визначене радіомоніторингом, не збігаються.

Нехай дослідження спектрів показало, що спектр випадкового сигналу збігається зі спектром з бази даних. В результаті декларується збіжність двох спектрів. Виникає питання, Чи дійсно у такому випадку випадковий сигнал є сигналом засобу негласного отримання інформації? За теоремою Байєса апостеріорна ймовірність того, що спектр сигналу є спектром сигналу засобу негласного отримання інформації за збіжністю спектрів сигналів:

$$p(C \mid M) = \frac{p(M \mid C)p(C)}{p(M \mid C)p(C) + p(M \mid \bar{C})p(\bar{C})}. \quad (1)$$

Введемо позначення: p_{CA} – апріорна ймовірність події C, тобто, апріорну ймовірність події $p(C)$ і запишемо теорему у вигляді:

$$p(C \mid M) = \frac{p(M \mid C)p_{CA}}{p(M \mid C)p_{CA} + p(M \mid \bar{C})(1 - p_{CA})} = \\ = \frac{p(M \mid C)p_{CA}}{p(M)}. \quad (2)$$

Оскільки:

$$p(\bar{C} \mid M) = \frac{p(M \mid \bar{C})(1 - p_{CA})}{p(M \mid \bar{C})(1 - p_{CA}) + p(M \mid C)p_{CA}}, \quad (3)$$

то апостеріорний шанс того, що спектр сигналу не є спектром сигналу засобу негласного отримання інформації, прийме вигляд:

$$\frac{p(\bar{C} \mid M)}{p(C \mid M)} = \frac{p(M \mid \bar{C})}{p(M \mid C)} \times \frac{(1 - p_{CA})}{p_{CA}}, \quad (4)$$

де $\left[(1 - p_{CA}) / p_{CA}\right]$ – апріорний шанс того, що спектр сигналу не є спектром сигналу засобу негласного отримання інформації. З цього прикладу видно, що перевагою використання відношення шансів є те, що немає необхідності обчислювати безумовну ймовірність $p(M)$, тобто, немає необхідності обчислювати константу пропорційності (знаменник) в теоремі Байєса.

Для подальшого обґрунтування застосування теореми Байєса для виявлення сигналу засобів негласного отримання інформації, розглянемо фактор Байєса.

Фактор Байєса – це апостеріорний шанс того, спектр сигналу є спектром сигналу засобу негласного отримання інформації.

Оскільки $p(C \mid M) = 1 - p(\bar{C} \mid M)$, то можливо записати вираз для фактора Байєса у вигляді:

$$r = p(M \mid C) / p(M \mid \bar{C}) = \\ = p(M \mid C) / [1 - p(\bar{M} \mid C)], \quad (5)$$

який залежить тільки від даних. На основі виразу (5) отримаємо:

$$p(C \mid M) / p(\bar{C} \mid M) = p(M \mid C) / p(M \mid \bar{C}) \times \\ \times [p_{CA} / (1 - p_{CA})] = r[p_{CA} / (1 - p_{CA})], \quad (6)$$

де r – фактор Байєса, який являє собою апостеріорний шанс того, що спектр сигналу є спектром сигналу засобу негласного отримання інформації.

Таким чином, незалежно від значення p_{CA} , чим більшим буде фактор Байєса, тим більшим буде шанс на користь події C (спектр сигналу є спектром сигналу засобу негласного отримання інформації)). Зазначимо, що значення r залежить тільки від даних. В подальшому фактор Байєса буде використовуватись при перевірці гіпотез.

Тепер необхідно оцінити апріорну ймовірність p_{CA} того, що спектр сигналу є спектром сигналу засобу негласного отримання інформації. Для простоти обчислень, введемо припущення, а саме приймемо, що апріорна ймовірність p_{CA} = 0,5. У даному прикладі є ймовірності припуститись двох помилок:

1. $p(\bar{M} \mid C)$ – ймовірність прийти до висновку, що немає збіжності спектрів сигналів, якщо вона повинна бути;

2. $p(M \mid \bar{C})$ – ймовірність того, що є збіжність спектрів сигналів, коли її не має бути (припустимо, що сигнал – це випадковий сигнал, якій не є спектром сигналу засобу негласного отримання інформації).

Ці ймовірності визначаються поточним рівнем розвитку технології та точністю засобів, які проводять спектральний аналіз радіодіапазону, припустимо (за наявними статистичними даними), що $p(M \mid \bar{C}) = 0{,}03$, а $p(\bar{M} \mid C) = 0{,}002$.

Обчислення цих значень досить складне і залежить від результатів порівняння спектру випадкового сигналу з відповідної бази даних. Воно залежить також від результатів порівняння декількох незалежних характеристик спектра цих двох сигналів

Використовуючи наведені вище значення для $p(M \mid \bar{C})$, $p(\bar{M} \mid C)$, а також те, що $p(M \mid C) = 1 - p(\bar{M} \mid C) = 1 - 0{,}002 = 0{,}998$, обчислимо ймовірність того, що спектр сигналу є спектром сигналу засобу негласного отримання інформації:

$$p(\bar{C} \mid M) = \frac{p(M \mid C)\, p_{CA}}{p(M \mid C)\, p_{CA} + p(M \mid \bar{C})(1 - p_{CA})} = \\ = \frac{0{,}998 \times 0{,}5}{0{,}998 \times 0{,}5 + 0{,}03 \times 0{,}5} = 0{,}9708,$$

або біля 97%. Використовую вираз (5), знаходжу фактор Байєса, фактор Байєса $r = [p_{CA} / (1 - p_{CA})] = \frac{0{,}9708}{1 - 0{,}98708} = 33{,}36$. Апостеріорний шанс того, що спектр сигналу не є спектром сигналу засобу негласного отримання інформації:

$$\frac{1 - p(C \mid M)}{p(C \mid M)} = \frac{1 - 0{,}9708}{0{,}9708} = 0{,}0299 \approx 0{,}3$$

або апостеріорне свідчення на користь того, що спектр сигналу є спектром сигналу засобу негласного отримання інформації складає біля 33:1.

Таким чином, збіжність спектрів сигналів є, у даному випадку, переконливим доведенням того, що спектр випадкового сигналу отриманий при радіомоніторингу обраного радіодіапазону є саме сигналом засобу негласного отримання інформації.

Використання теореми Байєса для виявлення неправдивої інформації та блокування її розповсюдження у інформаційному просторі.

Для виявлення неправдивої інформації та блокування її розповсюдження у інформаційному просторі існують багато методів ідентифікації, для нашого випадку будемо використовувати тільки декілька з них, тобто зробимо припущення, що саме ці ознаки виявлення є головними. Застосуємо алгоритм та зробимо розрахунки. Нехай після проведеного аналізу інформації зроблена спроба виявити неправдиву інформацію. Ця інформація за оцінкою експертів є неправдивою (наприклад, надійшла з чат ботів, з заборонених Web-ресурсів і т. ін.). Припустимо, що ця інформація дійсно є неправдивою. Таким чином, цю інформацію треба перевірити, співставити з оцінкою за базовими методами. Застосуємо для розв'язку цієї задачі теорему Байєса.

Введемо в розгляд такі події:

– C – випадковий аналіз інформації показав наявність ознак неправдивої інформації;

– $\bar{C}$ – випадковий аналіз інформації не показав наявність ознак неправдивої інформації;;

– M – ознаки інформації, визначене експертами, збігаються;

– $\bar{M}$ – ознаки інформації, визначене експертами, не збігаються.

Нехай дослідження експертів показало, що ознаки неправдивості інформації збігається зі методами виявлення ознак неправдивої інформації даних. В результаті декларується збіжність інформації. Але треба з'ясувати, дійсно, що у такому випадку інформація є неправдивою? За теоремою Байєса апостеріорна ймовірність того, що інформація є неправдивою інформацією за збіжністю отриманого висновку та розрахунків за існуючими методами та методиками. Далі будемо використовувати запропонований нами алгоритм, а саме для нашого випадку запишемо вираз:

$$p(C \mid M) = \frac{p(M \mid C)\, p(C)}{p(M \mid C)\, p(C) + p(M \mid \bar{C})\, p(\bar{C})}. \quad (7)$$

Введемо позначення: p_{CA} – апріорна ймовірність події C, тобто, апріорну ймовірність події $p(C)$ і запишемо теорему у вигляді:

$$p(C \mid M) = \frac{p(M \mid C)\, p_{CA}}{p(M \mid C)\, p_{CA} + p(M \mid \bar{C})(1 - p_{CA})} = \\ = \frac{p(M \mid C)\, p_{CA}}{p(M)}. \quad (8)$$

Оскільки:

$$p(\bar{C}\,|\,M)=\frac{p(M\,|\,\bar{C})(1-p_{CA})}{p(M\,|\,\bar{C})(1-p_{CA})+p(M\,|\,C)p_{CA}}, \quad (9)$$

то апостеріорний шанс того, що інформація не є неправдивою інформацією, матиме вигляд:

$$\frac{p(\bar{C}\,|\,M)}{p(C\,|\,M)}=\frac{p(M\,|\,\bar{C})}{p(M\,|\,C)}\times\frac{(1-p_{CA})}{p_{CA}}, \quad (10)$$

де $\left[(1-p_{CA})/\,p_{CA}\right]$ – апріорний шанс того, що інформація не є неправдивою інформацією. З цього прикладу видно, що перевагою використання відношення шансів є те, що немає необхідності обчислювати безумовну ймовірність $p(M)$, тобто, немає необхідності обчислювати константу пропорційності (знаменник) в теоремі Байєса.

Для подальшого обґрунтування застосування теореми Байєса для виявлення неправдивої інформації, розглянемо фактор Байєса.

Фактор Байєса – це апостеріорний шанс того, інформація є неправдивою інформацією.

Оскільки $p(C\,|\,M)=1-p(\bar{C}\,|\,M)$, то можливо записати вираз для фактора Байєса у вигляді:

$$r=p(M\,|\,C)/\,p(M\,|\,\bar{C})=\\ =p(M\,|\,C)/[1-p(\bar{M}\,|\,C)], \quad (11)$$

який залежить тільки від даних. На основі виразу (11) отримаємо:

$$p(C\,|\,M)/\,p(\bar{C}\,|\,M)=p(M\,|\,C)/\,p(M\,|\,\bar{C})\times\\ \times[p_{CA}/(1-p_{CA})]=r[p_{CA}/(1-p_{CA})], \quad (12)$$

де r – фактор Байєса, який являє собою апостеріорний шанс того, інформація є неправдивою. Таким чином, незалежно від значення p_{CA}, чим більшим буде фактор Байєса, тим більшим буде шанс на користь події C (інформація буде неправдивою). Зазначимо, що значення r залежить тільки від даних. В подальшому фактор Байєса буде використовуватись при перевірці гіпотез.

Тепер необхідно оцінити апріорну ймовірність p_{CA} того, інформація є неправдивою. Для простоти обчислень, введемо припущення, а саме приймемо, що апріорна ймовірність $p_{CA}=0{,}5$.

У даному прикладі є ймовірності припуститись двох помилок:

1. $p(\bar{M}\,|\,C)$ – ймовірність прийти до висновку, що немає параметрів збіжності правдивості та неправдивості інформації, якщо вона повинна бути;

2. $p(M\,|\,\bar{C})$ – ймовірність того, що є збіжність параметрів збіжності правдивості та неправдивості інформації, коли її не має бути.

Ці ймовірності визначаються поточним рівнем розвитку технології та точністю засобів, які проводять аналіз інформації, припустимо (за наявними статистичними даними), що $p(M\,|\,\bar{C})=0{,}01$, а $p(\bar{M}\,|\,C)=0{,}001$.

Обчислення цих значень досить складне і залежить від результатів порівняння інформації з відповідної бази параметрів неправдивості інформації. Воно залежить також від результатів порівняння декількох незалежних ознак інформації цих двох ознак інформації

Використовуючи наведені вище значення для $p(M\,|\,\bar{C}),\ p(\bar{M}\,|\,C)$, а також те, що $p(M\,|\,C)=1-p(\bar{M}\,|\,C)=1-0{,}001=0{,}999$, обчислимо ймовірність того, інформація є неправдивою:

$$p(\bar{C}\,|\,M)=\frac{p(M\,|\,C)p_{CA}}{p(M\,|\,C)p_{CA}+p(M\,|\,\bar{C})(1-p_{CA})}=\\ =\frac{0{,}999\times0{,}5}{0{,}999\times0{,}5+0{,}01\times0{,}5}\approx0{,}9901,$$

або біля 99%. Використовую вираз (5), знаходжу фактор Байєса, фактор Байєса $r=[p_{CA}/(1-p_{CA})]=\frac{0{,}9901}{1-0{,}9901}\approx99{,}999$. Апостеріорний шанс того, що інформація не є неправдивою інформацією:

$$\frac{1-p(C\,|\,M)}{p(C\,|\,M)}=\frac{1-0{,}9901}{0{,}9901}=0{,}099\approx\frac{1}{10},$$

або апостеріорне свідчення на користь того, що інформація, яка підлягає аналізу є неправдивою та складає біля 10:1.

Таким чином, у даному випадку, переконливим доведенням того, що інформація яка підлягає аналізу є саме неправдивою інформацією.

ВИСНОВКИ

У роботі запропоновано алгоритм практичного застосування теореми Байєса до виявлення небезпеки у системах інформаційної безпеки. Математичними розрахунками доведено доцільність використання теореми Байєса для виявлення порушення конфіденційності та правдивості інформації. За результатами розрахунків з використанням конкретних припущень отримали апостеріорне свідчення на користь того, що спектр сигналу є спектром сигналу засобу негласс-

ного отримання інформації складає біля 33:1, а для визначення неправдивої інформації апостеріорний шанс того, що інформація не є неправдивою інформацією 10:1, це є гарними результатами. Таким чином довели, що використання теореми Байєса для визначення захищеності інформації за запропонованим алгоритмом є удосконаленням методу оцінки захисту інформації та дозволяє вирішувати наукове завдання по підвищенню ефективності інформаційної безпеки.

Напрямком подальших досліджень є завдання оптимізації критеріїв оцінки для підвищення ефективності інформаційної безпеки.

ЛІТЕРАТУРА

[1]. Лаптєва Т. О., Лукова-Чуйко Н.В. Удосконалення методу виявлення неправдивої інформації на основі методу експертної оцінки «Дельфі». Наукоємні технології. Том 55 № 3 (2022) С. 193-199. DOI: 10.18372/2310-5461.55.16901.

[2]. Boryseiko, O.; Laptiev, O.; Perehuda, O.; Ryzhov, A. Optimizing Energy Conversion in a Piezo Disk Using a Controlled Supply of Electrical Load. Axioms 2023, 12, 1074. https://doi.org/10.3390/axioms12-121074.

[3]. Barabash O., Laptiev O., Grushina O. The conceptual model of the intelligent network. Сучасний захист інформації, No4 (56), 2023, pp. 1-9. https:// doi.org/ 10.31673/2409-7292.2023.030202.

[4]. Лаптєв О., Зозуля С. Метод виключення відомих сигналів при скануванні заданого радіодіапазону. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». Том 2 № 22 (2023). С. 31-38. https: // doi.org / 10.28925/2663-4023.2023. 22.3138.

[5]. Sobchuk V., Sobchuk A., Laptiev S., Laptieva T., Hrebennikov A., Bobrov S.Investingation of dynamic processes in information networks with the application neural networks. International independent scientific journal. Poland. Vol.1, №26, 2021. pp.36-42.

[6]. Sobchuk V., Breslavsky V., Laptiev S., Laptieva T., Zahynei A., Kovalenko O. Development of routing algoritm for self-organizing information networks. German International Journal of Modern Science №7, Vol. 2, 2021. pp. 32-35, ISSN (Print) 2701-8369, ISSN (Online) 2701-8377.

[7]. Замрій І.В., Собчук А.В., Лаптєв С.О., Лаптєва Т.О., Копитко С.Б. Алгоритм контролю та прогнозування функціональної стійкості складних інформаційно-технічних систем. Телекомунікаційні та інформаційні технології. № 1 (74). 2022. С. 4-15.

[8]. Laptiev O., Lukova-Chuiko N., Laptiev S., Laptieva T., Savchenko V., Yevseiev S. Development of a method for detecting deviations in the nature of traffic from the elements of the communication network. International Scientific and Practical Conference "Information Security and Information Technologies": Conference Proceedings. 13-19 September 2021. Kharkiv Odesa, Ukraine. pp. 1-9, ISBN 978-966-676-818-9.

[9]. Lukova-Chuiko, N., Herasymenko, O., Toliupa, S., Laptieva, T., Laptiev, O. The method detection of radio signals by estimating the parameters signals of eversible Gaussian propagation. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021, Proceedings, 2021, C. 67-70, Scopus.

[10]. Тетяна Лаптєва. Алгоритм визначення міри існування недостовірної інформації в умовах інформаційного протиборства. Кібербезпека: освіта, наука, техніка. No 2 (14), 2021, С. 15-25. DOI 10. 28925/2663-4023.2021.14.1525

[11]. Тетяна Лаптєва. Алгоритм визначення міри існування недостовірної інформації в умовах інформаційного протиборства. Кібербезпека: освіта, наука, техніка. No 2 (14), 2021, С. 15-25. DOI 10. 28925/2663-4023.2021.14.1525.

[12]. Лаптєва Т.О. Методика виявлення неправдивої інформації для безпеки Держави. Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Об'єднані наукою: перспективи міждисциплінарних досліджень» 23-24 листопада 2023 р. Київ. Україна. С. 131-132.

[13]. Volodymyr Petrivskyi, Viktor Shevchenko, Serhii Yevseiev, Oleksandr Milov,Oleksandr Laptiev, Oleksii Bychkov, Vitalii Fedoriienko, Maksim Tkachenko, Oleg Kurchenko, Ivan Opirsky. Development of a modification of the method for constructing energy-efficient sensor networks using static and dynamic sensors. Eastern-European journal of enterprise technologies. Vol.1№9 (115), 2022 pp. 15-23. ISSN (print) 1729 - 3774. ISSN (on-line) 1729-4061. DOI: 10.15587/1729-4061.2022.252988, Scopus.

[14]. Лукова-Чуйко Н.В., Лаптєв О.А., Барабаш О.В., Мусієнко А.П., Ахрамович В.М. Метод розрахунку захисту персональних даних з урахуванням комплексу специфічних параметрів соціальних мереж. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. Київ: ВІКНУ, 2022. № 76. С. 54-68. https: // doi.org / 10.17721 / 2519-481X/ 2022/76-05.

[15]. V.Mukhin, V.Zavgorodnii, O.Barabash, R. Mykolaichuk, Y. Kornaga, A. Zavgo-rodnya, V. Statkevych, Method of Restoring Parameters of Information Objects in a Unified Information Space Based on Computer Networks, International Journal of Computer Network and Information Security (IJCNIS), 2020, vol.12 (2), pp. 11-21.

[16]. Buryachok V.L., L.V.Buryachok, V.V. Semko. The technology of the porous analog analysis and the evaluation of the occupancy of automated information systems. Science and Technology Journal of Modern Economic Informatics State University Telecommunications. Number 4, 2016, pp. 15-20.

[17]. Roman Kyrychok, Oleksandr Laptiev, Rostyslav Lisnevsky, Valeri Kozlovsky, Vitaliy Klobukov. Development of a method for checking vulnerabilities of a corporate network using bernstein transformations. Eastern-European journal of enterprise technologies. Vol.1№9 (115), 2022, pp. 93-101. ISSN (print) 1729-3774. ISSN (on-line) 1729-4061. DOI: 10.15587/1729-4061.2022.253530.

ALGORITHM FOR APPLICATION OF BAYES' THEOREM FOR DETECTION OF THREATS IN INFORMATION SECURITY SYSTEMS

Information protection is becoming more relevant in today's world. This is due to the growth of technical progress and the transformation of the world into an information world. This became especially noticeable after the worldwide quarantine from the corona virus, humanity generally switched to information communication. Social networks and, in general, information communication through the worldwide network of Internet cyberspace have acquired further development. In connection with this, the scientific task of developing new and improving existing methods of information protection arises. One of the ways to improve information protection is the application of Bayes' theorem. The paper proposes the practical application of Bayes' theorem to increase the effectiveness of danger detection in the information protection and information security system of the State. Mathematical calculations proved the expediency of using Bayes' theorem to detect violations of confidentiality and truthfulness of information. According to the results of calculations using specific assumptions, we received posteriori evidence in favor of the fact that the spectrum of the signal is the spectrum of the signal of a means of secretly obtaining information is about 33:1, and for determining false information, the a posteriori chance that the information is not false information is 10:1, that is are good results. In this way, it was proved that the use of Bayes' theorem to determine the security of information according to the proposed algorithm is an improvement of the method of assessing information protection and allows solving the scientific task of increasing the effectiveness of information protection and information security of the State.

Keywords: algorithm, nonlinear system, stability, delay, forecasting, information technologies, false information, personal data.

Глухов Сергій Іванович, доктор технічних наук, професор, Завідувач кафедри військово-технічної підготовки факультету післядипломної освіти Військового інституту, Київський національний університет імені Тараса Шевченка, Київ, Україна.
Serhiy Gluhov, Doctor of Technical Science, professor, Head of the Department of Military and Technical Training of the Faculty of Postgraduate Education of the Military Institute, Taras Shevchenko National University of Kyiv.
E-mail: gluhov1971@ukr.net.
Orcid ID: 0000-0002-4918-3739.

Половінкін Ігор Михайлович, кандидат військових наук, снс, Директор Науково-методичного центру кадрової політики МО України.
Igor Polovinkin, Candidate of Military Sciences, Senior Researcher, Director of the Scientific and Methodological Center for Personnel Policy of the Ministry of Defense of Ukraine.
E-mail: Igor1964mo@i.ua.
Orcid ID: 0000-0003-0141-0274.

Кузьменко Максим Дмитрович, кандидат психологічних наук, Науково-методичний центр кадрової політики МО України.
Maksym Kuzmenko, Candidate of Psychological Science, Scientific and Methodological Center for Personnel Policy of the Ministry of Defense of Ukraine.
E-mail: kyzmenko.m.d@gmail.com.
Orcid ID: 0000-0001-9204-979X.

Пономаренко Віталій Валерійович, аспірант навчально-наукового інституту захисту інформації, Державний університет інформаційно - комунікаційних технологій.
Vitaly Ponomarenko, PhD student of the educational and scientific institute of information protection, State University of Information and Communication Technologies
E-mail: Ur_suviator@ukr.net.
Orcid ID: 0000-0002-6567-4247.

DOI: 10.18372/2410-7840.26.18835
УДК 004.056.5

МАТЕМАТИЧНІ ОСНОВИ АЛГЕБРАЇЧНИХ РЕШІТОК ТА ЇХ ЗАСТОСУВАННЯ В КВАНТОВІЙ КРИПТОЛОГІЇ

Андрій Кожухівський, Олександр Хіміч, Олександр Потій, Юрій Горбенко, Ольга Кожухівська, Юрій Борсуковський

Постійний розвиток квантових комп'ютерів загрожує найсучаснішим криптографічним схемам з відкритим ключем, таким як схеми генерації ключів на основі факторизації дискретних логарифмів, цифрових підписів та криптографії на еліптичних кривих. Необхідно розробляти нові криптографічні алгоритми, здатні протистояти атакам квантових комп'ютерів. Постквантова криптографія (PQC) спрямована на розробку алгоритмів, які можна використовувати без значних модифікацій існуючих мереж. Національний інститут стандартів і технологій США (NIST) організовує конкурс для відбору і стандартизації нових алгоритмів. Ця стаття містить огляд та аналіз процесу оцінки та відбору алгоритмів NIST на основі