between automated robotic systems. Nevertheless, information technologies have transformed the nature of war and continue to do so. Military doctrines and combat rules, previously developed, need to be updated to address current and future challenges. The integration of information technologies with armed conflict has not only changed the arsenal of available weapons but also blurred the lines between the physical and cyber domains. Traditional military arsenals, once dominated by tanks, aircraft, and infantry, are now supplemented by powerful cyber capabilities. Modern cyberattack landscapes allow for penetration into the information systems of both military targets and critical state infrastructure, significantly expanding the scope of influence. The rapid development of the cyber domain requires the development of an effective methodological approach to the cyber protection of critical infrastructure objects (CIOs). To enhance the cybersecurity level of these vital objects, analyze current cyber threats, forecast the likelihood of enemy cyberattacks, and implement protection mechanisms for the information and communication systems of CIOs, it is essential to assess the CIOs' capabilities to maintain functionality under destructive cyber influences and to restore operations after interference with the information and communication systems of CIOs. Developing recommendations for tools to assess cyber resilience will enhance the security and protection level of critical infrastructure under national security threats.

Keywords: cybersecurity, cyber resilience, cyber defense, information systems, cyber protection, information and telecommunication systems, resilience, critical infrastructure objects, assessment, technology, network security, national security, hybrid threats, evaluation, methodological approach, methodology, system, threats to national security, modeling, mathematical model.

Шиповський Володимир Володимирович, ад'юнкт кафедри інформаційно-аналітичних технологій Інституту інформаційно-телекомунікаційних технологій та кібероборони Національного університету оборони України імені Івана Черняховського.

Volodymyr Shypovskyi, adjunct of the Department of Information and Analytical Technologies of the Institute of Information and Telecommunication Technologies and Cyber Defense of the National Defense University of Ukraine named after Ivan Chernyakhovsky.
E-mail: stratcom.ndl@gmail.com.
Orcid ID: 0000-0003-3743-3064.

DOI: 10.18372/2410-7840.26.18827
УДК 336.71:004.056

МОДЕЛЬ ТОЧНОСТІ ПРОГНОЗУ ВИЯВЛЕННЯ НЕПРАВДИВОЇ ІНФОРМАЦІЇ У РЕАЛЬНОМУ ЧАСІ

Сергій Зибін, Андрій Собчук, Володимир Ровда

Інформаційна безпека Держави це актуальне завдання для країни яка проводить військові дії. Забезпечення інформаційної безпеки Держави актуальне наукове завдання для усіх країн. Проблема інформаційного протиборства, інформаційна війна завжди займала першочергове місце у загальної безпеки Держави. За допомогою злочинного інформаційного впливу можливо керувати соціумом, суспільним настроїм. Тому розробка та удосконалення науково-методичного апарату, а саме розробка моделі точності прогнозу виявлення неправдивої інформації у реальному часі, як засіб введенню інформаційного протиборства, є актуальним науковим завданням. Вирішенню цього наукового завдання і присвячена дана наукова робота. У роботі досліджується математичний апарат виявлення та блокування неправдивої інформації у реальному часі. Саме вирішенню проблеми виявлення неправдивої інформації і присвячена стаття. Розглянута ситуація, коли реконструйований сигнал генерується моделлю Мандельброта, далі використовую метод самонавчання Кохонена. Уточнюючі невідомі параметри за допомогою стандартного метода Утадроу – Хоффа отримали модель точності прогнозу виявлення неправдивої інформації. Яка дозволяє виявляти неправдиву інформації у реальному часі. Напрямком подальших досліджень може бути завдання оптимізації критеріїв оцінки точності прогнозу.

***Ключові слова**: неправдива інформація, виявлення, блокування, реальний час.*

ВСТУП

Для вирішення задачі виявлення та блокування розповсюдження неправдивої інформації необхідно розуміти принципи, за якими вона поширюється. В цьому допомагають методи комп'ютерної лінгвістики для того, щоб зрозуміти правила та шаблони, за якими можна ідентифікувати елементи дезінформації в потоці текстових даних. Дослідження показали, що для створення фейкової інформації набір тексту використовується за певними правилами, щоб новина здавалася правдивою [1]. Неправдивий контент має певні особливості, такі як скорочення, передача меншої кількості інформації, негативний характер. Також прослідковуються елементи не аналітичної думки, а більш неформального мислення. Особливістю інформаційної загрози є поява тенденції до багаторазового сталого повто-

рення в новинах та коментарях до них певної теми (сукупності взаємопов'язаних тем), спрямованої на дискредитацію об'єкта інформаційної атаки. Виявити загрозу – це виявити наявність відповідних тенденцій, пов'язаних з її формуванням.

Дослідження точності виявленням неправдивої інформації може здійснюватися на різних рівнях: пунктуаційному, орфографічному, синтаксичному, лексико- фразеологічному та стилістичному. Найбільший інтерес дослідників представляє аналіз трьох останніх рівнів. Існує доволі багато методів аналізу стилю. В цілому їх можна розділити на дві групи: експертні та формальні. Експертні методи аналізу є доволі трудомісткими. Формальні методи базуються на алгоритмах статистичного аналізу, машинного навчання, нейронних мереж, Text mining та ін. Останнім часом зростає популярність методів вбудовування в мережі (embedded networks). Інформація моделюється як мережа, що складається з вузлів та зв'язків між ними. Зважаючи на широкий спектр методів та труднощів в задачах визначення авторства, актуальною науково-практичною задачею є аналіз та практична реалізація цих методів, що можуть бути використані для створення автоматизованих систем визначення авторства.

ПОСТАНОВКА ПРОБЛЕМИ

На сучасний момент, коли іде війна з рашистами, вирішення задачі виявлення та блокування неправдивої інформації стає дуже гостро. Тому, що це безпосереднє впливає на інформаційну безпеку Держави. Інформаційна безпека Держави це актуальне завдання для країни яка проводить військові дії. Тому розробка та удосконалення науково-методичного апарату, а саме розробка моделі точності прогнозу виявлення неправдивої інформації у реальному часі є актуальним науковим завданням. Вирішенню цього наукового завдання і присвячена дана наукова робота.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Забезпечення інформаційної безпеки Держави в умовах сучасного інформаційного життя являється чи не найважливішим аспектом у задоволенні безпечного використання усіх можливостей нинішніх технологій.

У роботі [1] розглядається головні аспекти протиборства. Ситуація ускладняється великій кількістю джерел інформації та обмеженості джерел правдивої інформації. Інформація може бути суб'єктивною та упередженою, ці властивості складають сутність інформаційного протиборства, коли протидіючі сторони намагаються будь-що чинити інформаційний тиск як на джерела інформації так і на увесь процес її розповсюдження.

Для забезпечення нормального функціонування, прийняття адекватних рішень завданням кінцевого користувача є одержання об'єктивної своєчасної інформації, для чого на передній план виступають питання оцінювання її достовірності. Але властивості інформації не розглядаються.

У роботах [2, 3, 7] обговорюється загрози інформаційної безпеки Держави. Наводиться, що під загрозою інформаційної безпеки розуміється потенційно можлива подія, процес або явище, яке за допомогою негативного впливу на інформацію може прямо або опосередковано призвести до порушення цілісності цієї інформації, а також має можливість впливу на компоненти інформаційно-комунікаційних систем, що призводить до їх втрати, знищення або збою функціонування, тим самим наносячи шкоду інтересам суб'єктів інформаційних відносин. Але закони розповсюдження інформації не набули розкриття у цих джерелах.

У роботах [4-6, 9] обговорюється суть та аналіз інформації. Інформація це та суть, яку не можна поторкати, а значить на неї не поширюються деякі, звичні нам правила і закони. Аналіз можливо визначити як діяльність по вивченню великої кількості даних, висновки по стану справ зараз, побудові прогнозів на основі цих даних і виробленню рекомендацій. Але аналіз обмежується лише осмислюванням отриманих даних з метою обґрунтовано відповісти на наступні питання: яка ситуація зараз, як розвиватимуться події; яка можлива шкода або можлива користь; як використати нові можливості або запобігти негативу.

У роботах [8, 10-12, 14] робиться акцент на те, що ми постійно займаємося аналізом інформації. Загалом нова інформація викликає різні процеси, які дозволяють нам оцінити доведену нам інформацію, зіставити з наявною, зробити висновки і т.п. у роботі наведені основні питання інформаційного аналізу. Що відбувається, коли ви отримуєте нову порцію інформації? Які процеси виникають у вашій голові? Які процеси є основними які другорядними? Погодьтеся, це не просто, хоча кожен з нас цим займається щомиті. Навіть коли ми спимо наш мозок здійснює ці процеси, хай і в зменшеному, в порівнянні з активною фазою, об'ємі. Але шляхи та алгоритми аналізу інформації не наводяться.

Разом з тим, незважаючи на значну кількість публікацій щодо вирішення різноманітних аспектів існування інформації в умовах інформаційного протиборства оцінювання достовірності інформації на сьогоднішній день залишається невирішеною проблема комплексного оцінювання достовірності інформації.

Тому розробка та удосконалення науково-методичного апарату, а саме розробка моделі точності прогнозу виявлення неправдивої інформації у реальному часі є актуальним науковим завданням.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

При аналізі великого обсягу інформації, складним завданням є динамічна реконструкція, що полягає у відновленні моделі, що генерує досліджуваний часовий ряд, за вибіркою $x(1), x(2), \ldots, x(k), \ldots$. При цьому подібно до класичного завдання ідентифікації [16, 17] ця проблема може розглядатися в двох аспектах: параметрична реконструкція, коли структура моделі задана, а потрібно відновити її параметри, і структурна, коли апріорі не відомі ні структура, ні параметри моделі.

Розглянемо спочатку ситуацію, коли реконструйований сигнал генерується моделлю Мандельброта:

$$x_c(k+1) = x_c^2(k) + \theta, \tag{1}$$

$$\begin{cases} x_c(k) = x_1(k) + ix_2(k), \\ \theta = \theta_1 + i\theta_2, \quad i = \sqrt{-1}. \end{cases} \tag{2}$$

Передбачається, що параметри θ_1 та θ_2 невідомі.

Переписавши (1) у вигляді:

$$\begin{aligned} \vec{x}(k+1) &= \begin{pmatrix} x_1(k+1) \\ x_2(k+1) \end{pmatrix} = \\ &= \begin{pmatrix} x_1^2(k) - x_2^2(k) \\ 2x_1(k)x_2(k) \end{pmatrix} + \begin{pmatrix} \theta_1 \\ \theta_2 \end{pmatrix} = \\ &= \begin{pmatrix} \psi_1(x_c(k)) \\ \psi_2(x_c(k)) \end{pmatrix} + \begin{pmatrix} \theta_1 \\ \theta_2 \end{pmatrix} = \vec{\psi}\left(x_c(k)\right) + \vec{\theta}, \end{aligned} \tag{3}$$

ввівши вектор помилок:

$$\begin{aligned} \vec{e}(k) &= \begin{pmatrix} e_1(k) \\ e_2(k) \end{pmatrix} = x(k)I_2 - \vec{x}(k) = \\ &= x(k)I_2 - \vec{\psi}\left(x_C(k-1)\right) - \vec{\theta}, \end{aligned} \tag{4}$$

та критерій навчання:

$$E(k) = \frac{1}{2}\left\|\vec{e}(k)\right\|^2 = \frac{1}{2}\left\|\tilde{x}(k) - \vec{\theta}\right\|^2. \tag{5}$$

Можливо записати рекурентний метод його мінімізації у вигляді:

$$\vec{\theta}(k+1) = \vec{\theta}(k) + \eta(k)\left(\tilde{x}(k) - \vec{\theta}(k)\right), \tag{6}$$

$$\tilde{x}(k) = x(k)I_2 - \vec{\psi}\left(x_c(k-1)\right), \quad I_2 = (1,1)^T. \tag{7}$$

Нескладно бачити, що формула (7) збігається з методом самонавчання Кохонена, при цьому відновлені параметри дозволяють отримати пару прогнозних значень ряду, що спостерігається у вигляді:

$$\hat{\tilde{x}}(k+1) = \vec{\psi}\left(x_c(k)\right) + \vec{\theta}(k+1). \tag{8}$$

Розглянемо далі складнішу структуру комплексного процесу:

$$\begin{aligned} \vec{x}(k+1) &= \begin{pmatrix} x_1(k+1) \\ x_2(k+1) \end{pmatrix} = \\ &= \begin{pmatrix} w_{11}\left(x_1^2(k) - x_2^2(k)\right) + \theta_1 \\ w_{21}x_1(k)x_2(k) + \theta_2 \end{pmatrix} = \\ &= \begin{pmatrix} w_{11}\psi_1\left(x_c(k)\right) + \theta_1 \\ w_{21}\psi_2\left(x_c(k)\right) + \theta_2 \end{pmatrix} = \\ &= \begin{pmatrix} w_{11} & \theta_1 \\ w_{21} & \theta_2 \end{pmatrix} \times \begin{pmatrix} \psi_1\left(x_c(k)\right) & 1 \\ \psi_2\left(x_c(k)\right) & 1 \end{pmatrix} I_2 = \\ &= W \times \Psi\left(x_c(k)\right) I_2, \end{aligned} \tag{9}$$

Переписавши (9) по компонентне:

$$\begin{cases} x_1(k+1) = \left(w_{11}, \quad \theta_1\right)\left(\psi_1(x_c(k)), \quad 1\right)^T = \\ = w_1\Psi_1\left(x_c(k)\right), \\ x_2(k+1) = \left(w_{21}, \quad \theta_2\right)\left(\psi_2(x_c(k)), \quad 1\right)^T = \\ = w_2\Psi_2\left(x_c(k)\right), \end{cases} \tag{10}$$

можливо уточнити невідомі параметри за допомогою стандартного метода Утадроу – Хоффа у вигляді:

$$\begin{cases} w_1(k+1) = w_1(k) + \\ \eta\dfrac{x(k) - w_1(k)\Psi_1\left(x_c(k-1)\right)}{1 + \psi_1^2\left(x_C(k-1)\right)}\Psi_1^T\left(x_C(k-1)\right), \\ w_2(k+1) = w_2(k) + \\ \eta\dfrac{x(k) - w_2(k)\Psi_2\left(x_c(k-1)\right)}{1 + \psi_2^2\left(x_c(k-1)\right)}\Psi_2^T\left(x_c(k-1)\right), \end{cases} \tag{11}$$

та на їх основі будувати пару одно крокових прогнозів:

$$\hat{\hat{x}}(k+1) = W(k+1) \odot \Psi\left(x_C(k)\right) I_2. \qquad (12)$$

де $\odot$ – символ скоттова множення.

Комплексний прогноз речового процесу $x(k)$ може бути деяким чином "згорнутий" з метою отримання більш точних результатів. Для цього можливо використовувати адитивну форму:

$$\hat{x}(k+1) = c\hat{x}_1(k+1) + \left(1-c\right)\hat{x}_2(k+1), \qquad (13)$$

де c – деякий параметр, що визначає точність прогнозування, $\hat{x}(k+1)$ – комплексний прогноз речового процесу $x(k)$.

Ввівши $\left(k \times 1\right)$ – вектори сигналів та помилок (14) та розв'язавши диференціальне рівняння (15) можливо отримати співвідношення (16):

$$\begin{cases} X(k) = \left(x(1), x(2), \ldots, x(k)\right)^T, \\ \hat{X}(k) = \left(\hat{x}(1), \hat{x}(2), \ldots, \hat{x}(k)\right)^T, \\ \hat{X}_i(k) = \left(\hat{x}_i(1), \hat{x}_i(2), \ldots, \hat{x}(k)\right)^T, \quad i = 1, 2, \\ V(k) = X(k) - \hat{X}(k), \\ V_i(k) = X(k) - \hat{X}_i(k), \quad i = 1, 2, \\ V(k) = cV_1(k) + (1-c)V_2(k), \end{cases} \qquad (14)$$

$$\frac{\partial \left\|V(k)\right\|^2}{\partial c} = 0, \qquad (15)$$

$$\begin{cases} c(k) = V_2^T(k) \dfrac{V_2(k) - V_1(k)}{\left\|V_2(k) - V_1(k)\right\|^2}, \\ 1 - c(k) = V_1^T(k) \dfrac{V_1(k) - V_2(k)}{\left\|V_1(k) - V_2(k)\right\|^2}. \end{cases} \qquad (16)$$

Підставивши (16) в останнє рівняння (14), отримаємо:

$$\begin{aligned} V(k) &= V_2^T(k) \frac{V_2(k) - V_1(k)}{\left\|V_2(k) - V_1(k)\right\|^2} V_1(k) + \\ &+ V_1^T(k) \frac{V_1(k) - V_2(k)}{\left\|V_1(k) - V_2(k)\right\|^2} V_2(k) = \\ &= \left(V_1(k)V_2^T(k) - V_2(k)V_1^T(k)\right) \frac{V_1(k) - V_2(k)}{\left\|V_1(k) - V_2(k)\right\|^2}. \end{aligned} \qquad (17)$$

З цього слідує

$$\begin{aligned} \left\|V(k)\right\|^2 = &\left(\left\| \begin{array}{l} \left(\left\|V_2(k)\right\|^2 - V_1^T(k)V_2(k)\right)V_1(k) + \\ + \left(\left\|V_1(k)\right\|^2 - V_1^T(k)V_2(k)\right)V_2(k) \end{array} \right\|^2 \right) \times \\ &\times \left\|V_1(k) - V_2(k)\right\|^{-4}. \end{aligned} \qquad (18)$$

Використовуючи (18), можливо отримати систему нерівностей

$$\begin{cases} \left\|V(k)\right\|^2 - \left\|V_1(k)\right\|^2 = \\ = -\dfrac{\left(\left\|V_1(k)\right\|^2 - V_1^T(k)V_2(k)\right)^2}{\left\|V_1(k) - V_2(k)\right\|^2} \le 0, \\ \left\|V(k)\right\|^2 - \left\|V_2(k)\right\|^2 = \\ = -\dfrac{\left(\left\|V_2(k)\right\|^2 - V_1^T(k)V_2(k)\right)^2}{\left\|V_1(k) - V_2(k)\right\|^2} \le 0, \end{cases} \qquad (19)$$

яка свідчить про те, що точність прогнозу (13) ніколи не може бути гірше, ніж точність за кожною з компонент (12).

Для роботи у реальному часі отримані співвідношення слідує представляти у рекурентному вигляді, що можливо зробити застосувавши нові змінні:

$$\begin{cases} V_{21}(k) = V_2(k) - V_1(k), \\ e_1(k+1) = x(k+1) - \hat{x}_1(k+1), \\ e_2(k+1) = x(k+1) - \hat{x}_2(k+1), \\ e_{21}(k+1) = e_2(k+1) - e_1(k+1) \end{cases} \qquad (20)$$

та переписати (16) у вигляді:

$$\begin{cases} c(k+1) = \dfrac{\eta(k)}{\eta(k+1)} c(k) + \\ + \dfrac{e_2(k+1)e_{21}(k+1)}{\eta(k+1)}, \\ \eta(k+1) = \eta(k) + e_{21}^2(k+1), \end{cases} \qquad (21)$$

$$\begin{cases} V_{21}(k) = \hat{X}_1(k) - \hat{X}_2(k), \\ e_{21}(k+1) = \hat{x}_1(k+1) - \hat{x}_2(k+1) \end{cases}. \qquad (22)$$

В кінці отримуємо:

$$\begin{cases} c(k+1) = \dfrac{\eta(k)}{\eta(k+1)} c(k) + \\ + \dfrac{e_2(k+1)\left(\hat{x}_1(k+1) - \hat{x}_2(k+1)\right)}{\eta(k+1)}, \\ \eta(k+1) = \eta(k) + \left(\hat{x}_1(k+1) - \hat{x}_2(k+1)\right)^2, \end{cases}$$

(23)

де c – деякий параметр, що визначає точність прогнозування; $\hat{x}(k+1)$ – комплексний прогноз речового процесу $x(k)$.

Вираз (23) це модель точності прогнозу виявлення неправдивої інформації у реальному часі. Яка є метою нашого дослідження.

ВИСНОВКИ

Провівши дослідження та розглянувши ситуацію, коли реконструйований сигнал генерується моделлю Мандельброта, використано метод самонавчання Кохонена, за допомогою якого відновлені параметри дозволяють отримати пару прогнозних значень ряду. Уточнюючі невідомі параметри за допомогою стандартного метода Утадроу – Хоффа отримали модель точності прогнозу виявлення неправдивої інформації. Яка дозволяє виявляти неправдиву інформації у реальному часі.

Напрямком подальших досліджень може бути завдання оптимізації критеріїв оцінки точності прогнозу.

ЛІТЕРАТУРА

[1]. Schefer-Wenzl, S., Strembeck, M. Modeling support for role-based delegation in process-aware information systems. Business and Information Systems Engineering. 6 (4). 2014. pp. 215-237. DOI: 10.1007 /s12599-014-0343-3.

[2]. 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, ISSN 2663-4023.

[3]. V. Savchenko, O. Laptiev, O. Kolos, R. Lisnevskyi, V. Ivannikova, I. Ablazov. Hidden Transmitter Localization Accuracy Model Based on Multi-Position Range Measurement. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. 2020. pp.246-251.

[4]. Valentyn Sobchuk, Volodymyr Pichkur, Oleg Barabash, Oleksandr Laptiev, Kovalchuk Igor, Amina Zidan. Algorithm of control of functionally stable manufacturing processes of enterprises. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp. 206-211.

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

[6]. Andrii Sobchuk, Halyna Haidur, Serhii Laptiev, Tetiana Laptieva, Farhod Asrorov, Oleh Perehuda. Modified Fourier transform for improving spectral analysis of radio signals. "Modern information, measurement and control systems: problems, applications and perspectives'2022" (MIMCS'2022). November 4-5, 2022, Antalya, Turkey.

[7]. Yevseiev, S., Trakaliuk, O., Kuzmenko, M., Laptieva T., Laptiev, S., Polovinkin, I. An Improved Method of Detection and Localization of Signals the Digital Range 2022 IEEE 4th International Conference on Advanced Trends in nformation Theory (ATIT), 15-17 December 2022, Kyiv, Ukraine, 2022. pp.129-132. DOI: 10.1109/ATIT58178.2022.10024242

[8]. 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.

[9]. 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: 10.15587/17-29-4061.2022.253530.

REAL-TIME FALSE INFORMATION DETECTION PREDICTION ACCURACY MODEL

State information security is an urgent task for a country conducting military operations. Ensuring the information security of the State is an urgent scientific task for all countries. The problem of information struggle, information war has always occupied a primary place in the general security of the State. With the help of criminal informational influence, it is possible to control society, public mood. Therefore, the development and improvement of the scientific and methodological apparatus, namely the development of a forecast accuracy model for the detection of false information in real time, as a means of introducing information warfare, is an urgent scientific task. This scientific work is devoted to the solution of this scientific task. The paper examines a mathematical apparatus for detecting and blocking false information in real time. The article is devoted to solving the problem of detecting false information. The situation is considered, when the reconstructed signal is generated by the Mandelbrot model, further using the Kohonen self-learning method. Specifying the unknown parameters using the standard Utadrow-Hoff method obtained a model of the accuracy of the prediction of false information detection. Which allows you to detect false information in real time. The direction of further research can be the task of optimizing the criteria for assessing the accuracy of the forecast.

Keywords: false information, detection, blocking, real time.

Зибін Сергій Вікторович, доктор технічних наук, професор кафедри безпеки інформаційних технологій Національного авіаційного університету, Київ, Україна.
Serhii Zybin, Doctor of technical sciences, professor of the department of security of information technologies National Aviation University, Kyiv, Ukraine.
E-mail: zysv@ukr.net.
Orcid ID: 0000-0002-2670-2823.

Собчук Андрій Валентинович, доктор філософії, доцент кафедри інформаційної та кібернетичної безпеки, Навчально-науковий інститут Захисту інформації, Державний університет телекомунікацій, Київ, Україна.
Andrii Sobchuk, PhD, Associate Professor of the Department of Information and Cyber Security, Educational and Scientific Institute of Information Protection, State University of Information and Communication Technologies.
E-mail: anri.sobchuk@gmail.com.
Orcid ID: 0000-0003-3250-3799.

Ровда Володимир Володимирович, аспірант, Державний університет інформаційно-комунікаційних технологій.
Volodymyr Rovda, PhD student, State University of Information and Communication Technologies.
E-mail: volodymyr.rovda@gmail.com.
Orcid ID: 0009-0001-9987-6787.

DOI: 10.18372/2410-7840.26.18829
УДК 004.49

ДОСЛІДЖЕННЯ ТА АНАЛІЗ ПРОБЛЕМ ТА ВИКЛИКІВ, ЩО ВИНИКАЮТЬ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ В ХМАРНИХ ОБЧИСЛЕННЯХ

Марта Король, Іван Опірський

Хмарні сервіси передбачають надання інформаційним засобам віртуального середовища можливість розширити програмно-технічні ресурси комп'ютерного пристрою користувача. При цьому інформація постійно зберігається на серверах у мережі Інтернет та тимчасово кешується на пристроях клієнтів, таких як персональні комп'ютери, ігрові консолі, ноутбуки, смартфони тощо. Для отримання постійного доступу до віддалених інтернет-ресурсів користувачі використовують хмарні сервіси. Вони є ключовим елементом сучасних технологій, які швидко розвиваються, а для багатьох компаній використання хмарних сервісів є стратегічним питанням. Хоча інноваційні можливості хмарних сервісів з одного боку привертають увагу користувачів, але з іншого можуть створювати нові загрози для їхньої інформаційної безпеки. Саме тому дослідження хмарних обчислень є важливим для розуміння їхнього потенціалу та ефективності. У цьому дослідженні буде розглянуто аспект безпеки хмарних сервісів, та порівняння декількох різних платформ в цьому контексті, адже відсутність достатнього захисту може призвести до крадіжки персональних даних та іншої конфіденційної інформації. В дослідженні також будуть розглянуті найпоширеніші загрози, з якими зіштовхуються хмарні сервіси, такі як DDoS-атаки, витоки даних, зловживання даними тощо. Зокрема, будуть проаналізовані заходи захисту, які надають провідні хмарні платформи, такі як AWS, GCP та Azure, з метою визначення їхньої ефективності та надійності. Наш аналіз буде корисним як для компаній, які розглядають можливість переходу до хмарних технологій, так і для звичайних користувачів, які прагнуть зберегти безпеку своїх особистих даних в Інтернеті. Результати дослідження нададуть чітке уявлення про переваги та обмеження використання різних хмарних платформ з точки зору безпеки.
Ключові слова: *хмарні сервіси, AWS, AZURE, GCP, кібербезпека.*

ВСТУП

В сучасному цифровому світі, великі обсяги даних зберігаються та оброблюються в хмарних сервісах. Відомо, що хмарні сервіси надають безліч переваг, включаючи збільшення доступності, гнучкість та економічність. Проте, разом з цими перевагами приходить ряд викликів, таких як збільшення загроз безпеці, потенційна вразливість та потенційні ризики для конфіденційності даних.

На даний момент, на ринку хмарних обчислень відбувається зростанням конкуренції серед провайдерів хмарних сервісів. За останні роки спостерігається постійне збільшення кількості компаній, що пропонують хмарні послуги. Найбільш популярними з них є:

1. Amazon Web Services (AWS) [2], (створена у березні 2006р.), є підрозділом компанії Amazon.com, яка пропонує хмарну обчислювальну платформу в оренду для приватних осіб, компаній та урядів за підпискою;

2. Microsoft Azure (створена 1 лютого 2010 р.) [3] – це інфраструктура корпорації Microsoft, яка надає хмарну платформу для розробників додатків, з метою полегшення процесу створення онлайн програм. Microsoft Azure дозволяє розго-