УДК 004.056

А. О. Азарова
І. А. Смоляк

Інформаційна технологія для оцінювання вразливостей інформаційної безпеки сучасних ІС

Вінницький національний технічний університет

Анотація

Розроблено ІТ для оцінювання вразливості рівня інформаційної безпеки сучасних ІС за допомогою штучного інтелекту. Запропоновано відповідну математичну модель та метод її формалізації на основі системного підходу та нейронної мережі Хеммінга. Це дозволяє оцінювати рівень вразливостей інформаційної безпеки досліджуваних ІС різних сфер застосування.

Ключові слова: вразливості інформаційної безпеки, штучний інтелект, нейронна мережа Хеммінга.

IT for assessment of information security vulnerabilities of modern informational systems

Abstract

The IT for assessing the vulnerability of the level of IS' information security by means of artificial intelligence has been developed. It is proposed an appropriate mathematical model and a method of its formalization based on a system approach and the Hamming neural network. IT makes possible to assess the level of information security vulnerabilities of the researched information systems in various application fields.

Keywords: information security's vulnerabilities, artificial intelligence, neural network of Hemming.

Вступ

Збільшення ресурсів для здійснення атак на інформаційні системи стає тенденцією, яка потребує постійної уваги та реалізації заходів їх ефективного захисту. Кіберзлочинці вдосконалюють свої методи та використовують різноманітні ресурси для покращення успішності атак. Згідно з офіційними даними провідних світових компаній, спеціалізованих у сфері кіберзахисту (Risk Based Security, McAfee Labs, Cybersecurity Education & Training Solutions, Mitre та ін.), протягом першої половини 2023 року було зафіксовано 2967 випадків витоку даних, при цьому до рук зловмисників потрапило 18,751 мільярда особистих записів юридичних та фізичних осіб. Серед зазначених випадків варто відзначити, що соціальна мережа Facebook втратила 533 мільйони записів, американський постачальник рецептурних препаратів CVSHealth – 1,16 мільярда записів, а міжнародна брокерська компанія FBS Markets Inc. – 16 мільярдів записів [1–4].

Отже, ідентифікація вразливостей сучасних ІС та, відповідно, подальше розроблення методів їх захисту є надзвичайно актуальним.

Результати дослідження

Сьогодні існує великий теоретичний доробок, який уможливлює реалізацію процесів захисту інформації. Серед провідних дослідників пошуку вразливостей інформаційної безпеки та захисту інформації треба відзначити таких закордонних, як Альгарті А., Джешке С., Каббас А., Мунші А., а також вітчизняних Архіпов О. Є., Вознюк Є. В., Карпінець В. В., Ромака В. А., Яремчук Ю. Є. та ін. дослідників [5-8]. Незважаючи на те, що є значний теоретичний та практичний доробок в досліджуваній галузі знань, слід відзначити що не всі питання ретельно висвітлено в науковій літературі, зокрема, не наводиться обґрунтована множина вразливостей ІС, яка б відповідала критеріям повноти, мінімальності і дієвості, що не дозволяє здійснити об'єктивне та точне оцінювання і, як наслідок сформувати ефективну систему засобів боротьби із кіберзлочинцями, що і зумовлює актуальність подальших досліджень у цьому напрямку.

Одним із інструментів для здійснення діяльності в сфері інформаційної безпеки є штучний інтелект (ШІ). Використання штучного інтелекту в інформаційній безпеці уможливлює значне підвищення ефективності захисту від кіберзагроз завдяки автоматизації процесів виявлення, аналізу та реагування на потенційні загрози. ШІ дозволяє оперативно виявляти аномалії у мережевому трафіку, розпізнавати нові види кібератак, ідентифікувати зразки шкідливого коду та здійснювати аналіз лог-файлів. Усі ці процеси відбуваються в режимі реального часу, допомагаючи зменшити час реакції на загрози, а також

усуваючи необхідність постійного нагляду людини. Такий підхід сприяє покращенню загального рівня безпеки інформаційних систем та даних, запобігає атакам та мінімізує можливі збитки внаслідок кіберінцидентів [9].

Отже, автори пропонують для побудови ІТ, що дозволяє оцінити рівень вразливості інформаційної безпеки ІС, застосовувати апарат ШІ, зокрема, мережу Хеммінга. Вона є потужним інструментом в арсеналі кібербезпеки для оцінювання та виявлення вразливостей інформаційних систем і мереж. Мережа використовує принципи аналізу нормальної поведінки системи та автоматизованого виявлення будь-яких відхилень від цієї норми. Використання нейронної мережі Хеммінга дозволяє отримати класифіковані та сегментовані дані, що визначають результат оцінювання рівня вразливості інформаційної безпеки ІС та, відповідно, встановити її тенденцію.

Процес перетворення множини первинних вхідних параметрів на множину вихідних рішень розглянемо у відповідній структурній моделі оцінювання вразливостей інформаційної безпеки ІС за допомогою нейронної мережі Хеммінга (рис. 1). Для побудови структурної та математичної моделі процесу оцінювання за критеріями повноти, мінімальності та дієвості сформуємо множину **A** оцінювальних параметрів $\{a_i, i=1,..,n$ та **B** вихідних рішень $b_j, j=1,..,m$.

Рис. 1 Структурна модель процесу оцінювання вразливості інформаційної безпеки ІС

Математична модель дозволяє відобразити множину $\mathbf{A}^*$ первинних вхідних параметрів a^*_k на множину **B** вихідних рішень b_j за допомогою реалізації функціоналів $\mathbf{C_1}$ та $\mathbf{C_2}$:

$$\mathbf{A}^* \xrightarrow{\mathbf{C_1}} \mathbf{A} \xrightarrow{\mathbf{C_2}} \mathbf{B},\ \mathbf{A}^* = \{a^*_k\},\ \mathbf{A} = \{a_i\},\ i=1,..,n,\ \mathbf{B}=\{b_j\},\ j=1,..,m,\ \mathbf{A} = \mathbf{C_1(A^*)},\ \mathbf{B} = \mathbf{C_2(A)}.$$

$$a_1 = f(a^*_1,\ldots a^*_3);\ a_2 = f(a^*_4,\ldots,a^*_6);\ a_3 = f(a^*_7,\ldots,a^*_9);\ a_4 = f(a^*_{10},\ldots,a^*_{12});\ a_5 = f(a^*_{13},\ldots,a^*_{15});$$
$$a_6 = f(a^*_{16},\ldots,a^*_{18});\ a_7 = f(a^*_{19},\ldots,a^*_{21});\ a_8 = f(a^*_{22},\ldots a^*_{24});\ a_9 = f(a^*_{25},\ldots,a^*_{27}).$$

Процес оцінювання значень параметрів a_i здійснюватимемо відповідним характеристичним термом із застосуванням авторського підходу, як запропоновано у табл. 1

Таблиця 1 – Присвоєння характеристичного терму, який описує значення параметра a_i

Назва оцінювального параметра a_i	Назва первинного вхідного параметра a^*_k	Характеристичний терм, який описує значення параметра a_i
a_1 – вразливості автентифікації та авторизації	a^*_1 – використання слабких паролів обсягом до 7 символів	В – високий рівень вираженості параметра a_i
	a^*_2 – використання паролів із низькою ентропією, таких як «password123» обсягом до від 7 до 9 символів	С – Середній рівень вираженості параметра a_i
	a^*_3 – використання паролів із високою ентропією, обсягом від 9 до 12 символів і більше	Н – Низький рівень вираженості параметра a_i
a_2 – вразливості захищеності веб-додатків	a^*_4 – відсутність механізмів безпеки веб-додатків	В
	a^*_5 – використання стандартних механізмів безпеки веб-додатків: HTTPS, OWASP, CORS, CSP	С
	a^*_6 – використання передових технік безпеки веб-додатків: WAF, XSS	Н
a_3 – вразливості керування доступом	a^*_7 – відсутність налаштувань рольового управління із обмеженням прав доступу (всі користувачі мають адміністративні привілеї)	В
	a^*_8 – використання рольового управління для об'єднаної групи користувачів	С
	a^*_9 – використання деталізованого рольового управління (застосування принципу найменших привілеїв)	Н
a_4 – вразливості шифрування даних	a^*_{10} – використання застарілих алгоритмів шифрування: DES, MD5, RSA, RC4	В
	a^*_{11} – використання стандартних алгоритмів шифрування, таких як AES або RSA, з ключами менше 128 біт для AES або менше 2048 біт для RSA	С
	a^*_{12} – використання сучасних алгоритмів шифрування з великою довжиною та унікальністю ключів, для AES з ключами довжиною 256 біт або RSA з ключами довжиною 3072 біт і більше	Н
a_5 – вразливості мережевої безпеки	a^*_{13} – відсутність брандмауерів	В
	a^*_{14} – використання брандмауерів для фільтрації та контролю трафіку типу WAF (Web Application Firewall)	С
	a^*_{15} – комплексне використання брандмауерів типу NGFW	Н
a_6 – вразливості фізичної безпеки	a^*_{16} – відсутність контролю доступу	В
	a^*_{17} – застосування контрольованого доступу	С
	a^*_{18} – застосування системи доступу на підставі біометричних показників	Н
a_7 – вразливості соціальної інженерії	a^*_{19} – відсутність проведення навчання персоналу з питань безпеки	В
	a^*_{20} – ситуативне проведення навчання персоналу з питань безпеки після інцидентів порушення інформаційної безпеки	С

	a^*_{21} – постійне проведення навчання персоналу з питань безпеки	Н
a_8 – вразливості системи виявлення та запобігання вторгнень	a^*_{22} – відсутність систем виявлення вторгнень	В
	a^*_{23} – використання звичайних систем виявлення вторгнень: IDS, IPS	С
	a^*_{24} – використання інтелектуальних систем з автоматичним реагування на загрози: SIEM, Palo Alto Networks Panorama	Н
a_9 – вразливості втрати даних	a^*_{25} – відсутність резервного копіювання даних	В
	a^*_{26} – резервне копіювання даних в ручному режимі	С
	a^*_{27} – автоматизоване резервне копіювання даних	Н

Реалізація функціоналу $\mathbf{C_2}$ полягає у відображенні множини **A** вхідних функцій a_i, закодовані значення яких подаються на вхід нейронної мережі Хеммінга, на множину **B** вихідних рішень b_j, j=1,..,m. Мережа Хеммінга для сигналу, поданого на її вхід, – закодованого вектора оцінювальних параметрів a_i знаходить відповідний еталонний зразок, що відповідає рівню вразливості інформаційної системи.

На рис. 1 подано структурну модель процесу оцінювання вразливості інформаційної безпеки із застосуванням системного підходу та нейронної мережі Хеммінга.

Шляхом використання експертних методів та проведення анкетного опитування серед фахівців з кібербезпеки щодо питань захисту інформаційних систем, було визначено граничні значення оцінювальних показників за трьома діапазонами: Н (низький), С (середній) та В (високий). Такий підхід дозволяє систематизувати інтервали значень для кожного оцінювального параметра a_i.

Розглянемо табл. 2, в якій експертами сформовано найбільш типові еталони для роботи мережі Хеммінга, вхідними параметрами якої є отримані на рівні 2 (див. рис. 1) значення оцінювальних параметрів a_i, що описуються характеристичними термами (Н, С, В) і кодуються, як описано нижче.

Таблиця 2. – Еталонні зразки нейронної мережі Хеммінга

№ еталону	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	b_j
1	Н	Н	Н	Н	Н	Н	Н	Н	Н	Н
2	Н	С	Н	Н	В	Н	Н	С	В	
3	С	С	С	С	С	С	С	С	С	С
4	Н	В	В	С	В	В	В	С	Н	В
5	В	В	В	В	В	В	В	В	В	

Оскільки нейронна мережа Хеммінга використовує тільки числові значення «1» та «-1», то автори пропонують закодувати значення 3 характеристичних термів – Н, С, В, що описують значення вхідних функцій a_i, відповідним двійковим кодом. Зауважимо, що формат коду, який складається з двох цифр, дозволяє закодувати навіть 4 (2^2=4) характеристичних терми.

Значення вихідних параметрів b_j (j=1,..3) оцінювання вразливостей інформаційної безпеки описується також трьома рівнями – Н (-1 -1), С (-1 1), В (1 1).

Використовуючи дані табл. 2, відобразимо закодовані еталонні набори значень показників вразливостей інформаційної безпеки, що подаються на вхід мережі Хеммінга так, як вказано у табл. 3.

Таблиця 3. Еталонні зразки для роботи мережі Хеммінга

№ еталона	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	b_j
1	-1-1	-1-1	-1-1	-1-1	-1-1	-1-1	-1-1	-1-1	-1-1	-1-1
2	-1-1	-1 1	-1-1	-1-1	1 1	-1-1	-1-1	-1 1	1 1	
3	-1 1	-1 1	-1 1	-1 1	-1 1	-1 1	-1 1	-1 1	-1 1	-1 1
4	-1-1	1 1	1 1	-1 1	1 1	1 1	1 1	-1 1	-1-1	1 1
5	1 1	1 1	1 1	1 1	1 1	1 1	1 1	1 1	1 1	

Використання мережі Хеммінга полягає у подаванні на її вхід вектору із 18 закодованих значень 9 оцінювальних параметрів a_i та порівняння цього вектору з найближчим до нього вектором із табл. 3 еталонів. Отже, нейронна мережа Хеммінга ідентифікує еталон, який є найближчим до вектора, поданого на її вхід. Номер даного еталону, що подано у табл. 3, дозволяє визначити результуюче рішення щодо

рівня вразливості інформаційної безпеки b_j (j = 1,…,3) ІС.

Таким чином, узагальнимо етапи реалізації функціоналів $\mathbf{C_1}$ та $\mathbf{C_2}$ запропонованої авторами структурної моделі, що представляються відповідними рівнями на рис.1:

Етап 1. Подання значення a^*_k (k=1,…27) первинних вхідних параметрів, що використовуються для розрахунку функцій (оцінювальних параметрів) a_i (i =1,…9) досліджуваних інформаційних систем;

Етап 2. Значення оцінювальних параметрів $a_1...a_9$ описуються конкретним характеристичним рівнем (Н – низький, С – середній, В – високий) шляхом реалізації функціоналу $\mathbf{C_1}$;

Етап 3. Формування вхідного вектору (який складається з 18 цифр «1» та «-1») для роботи мережі Хеммінга шляхом кодування значень оцінювальних параметрів a_i.

Етап 4. Нейронна мережа Хеммінга визначає найближчий до даного вектору еталон, номер якого відповідає певному вихідному рішенню b_j.

Роботу пропонованої авторами ІТ проілюструємо на етапі використання нейронної мережі Хеммінга для оцінювання рівнів вразливості інформаційної безпеки ІС, які застосовуються на 5 вітчизняних компаніях [10], що працюють у медичній та банківській сферах (табл. 4).

Таблиця 4 – Використання запропонованої ІТ для оцінювання вразливостей п’яти ІС у сфері медичних та банківських послуг

№ компанії	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	Рівень вразливості b_j
1	Н	В	В	С	В	В	В	Н	С	Високий
2	Н	С	В	С	С	С	С	С	С	Середній
3	В	Н	Н	С	Н	Н	Н	В	Н	Низький
4	Н	В	В	С	С	В	В	С	Н	Високий
5	Н	С	С	С	В	С	С	Н	С	Середній

Для перевірки адекватності складеної математичної моделі та методу її формалізації було порівняно результати, отримані за допомогою запропонованої авторами ІТ, застосованої на 5 суб’єктах господарювання (у сфері медичних та банківських послуг) із отриманими для цих компаній результатами за допомогою відомих на ринку ПЗ: Nessus, OpenVAS, Metasploit, Wireshark, Burp Suite, як розглянуто у табл. 5.

Таблиця 5 – Порівняння оцінок запропонованої ІТ із оцінками, отриманими засобами ПЗ: Nessus, OpenVAS, Metasploit, Wireshark, Burp Suite для ІС 5 компаній у сфері медичних та банківських послуг

ПЗ / № компанії	Рівень вразливості b_j за «Nessus»	Рівень вразливості b_j за «OpenVAS»	Рівень вразливості b_j за «Metasploit»	Рівень вразливості b_j за «Wireshark»	Рівень вразливості b_j за «Burp Suite»	**Рівень вразливості b_j за запропонованою ІТ**
1	В	В	В	В	В	В
2	С	С	С	С	С	С
3	Н	Н	Н	С	Н	Н
4	В	В	В	В	В	В
5	С	С	В	С	С	С

Отже, порівняння оцінок рівнів вразливостей 5 сучасних ІС, визначених за запропонованою ІТ та існуючими на ринку ПЗ, дозоляє отримати фактично однакові результати, що свідчить про адекватність складених математичної моделі та методу її формалізації, що автоматизовані засобами відповідної ІТ.

Висновки

Запропонована ІТ дозволяє комп’ютеризувати процедуру відображення обґрунтованої множини вхідних параметрів на множину вихідних рішень, що, на відміну від існуючих підходів, дозволяє засобами нейронної мережі Хеммінга значно підвищити точність такого процесу. Використання зазначеної ІТ дає такі переваги: забезпечення цілісності інформації, точність видачі результатів, захист від помилок, використання та врахування значної кількості оцінювальних параметрів, наявність елементів самостійного навчання, швидкість отримання результатів.

Отже, використання нейронних мереж для виявлення та оцінювання вразливостей інформаційної безпеки є передовим напрямком, що дозволяє ефективно впоратися зі складними викликами кібербезпеки. Ці технології автоматизують процес аналізу великих обсягів даних, розпізнають незвичайні патерни та реагують на потенційні загрози в режимі реального часу.

Застосування різних типів нейронних мереж дозволяє нам врахувати різноманітні аспекти безпеки, від розпізнавання візуальних аномалій до аналізу послідовностей даних. Їх гнучкість у пристосуванні до нових загроз та здатність до самонавчання роблять їх потужним інструментом в сфері кібербезпеки.

Застосування мережі Хеммінга в контексті оцінювання вразливостей інформаційної безпеки розкриває її можливості надійного виявлення помилок та відновлення цілісності даних. Це стає ключовим фактором для забезпечення надійності обміну інформацією в умовах постійних кібератак та технічних аномалій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cyber Risk Analytics. Security Ratings and Data Breach Intelligence. *Flashpoint* : веб-сайт. URL: https://flashpoint.io/wp-content/uploads/Flashpoint_Cyber_Risk_Analytics.pdf (дата звернення: 23.11.2023).
2. McAfee Labs Threats Reports. *McAfee* : веб-сайт. URL: https://www.mcafee.com/enterprise/ru-ru/threat-center/mcafee-labs/reports.html (дата звернення: 23.11.2023).
3. Cybersecurity Education & Training Solutions. 15 Alarming Cyber Security Facts and Stats. *ThriveDX* : веб-сайт. URL:https://www.cybintsolutions.com/cyber-security-facts-stats/ (дата звернення: 23.11.2023).
4. MITRE ATT&CK. *Attack.Mitre* : веб-сайт. URL: https://attack.mitre.org/ (дата звернення: 23.11.2023).
5. Kabbas A., Alharthi A, Munshi A. Artificial Intelligence Applications in Cybersecurity. *IJCSNS International Journal of Computer Science and Network Security*. VOL.20 No.2, Fabruary 2020. P. 120-124. URL: http://paper.ijcsns.org/07_book/202002/20200216.pdf (дата звернення: 23.11.2023).
6. Jeschke S. et al. Industrial Internet of Things and Cyber Manufacturing Systems. Cham. *Springer International Publishing Switzerland*. Vol. 3. 2017. P. 3–19. URL: https://link.springer.com/chapter/10.1007/978-3-319-42559-7_1 (дата звернення: 23.11.2023).
7. Яремчук Ю. Є., Карпінець В. В., Зоря І.С. Проблеми експлуатації та захисту інформаційно-комунікаційних систем. Тези науково-практичної конференції, м. Київ, 7 – 9 червня 2023 р., *Національний авіаційний університет. – К.: Вид-во НАУ*. 2023. 49-51 с. URL: https://iq.vntu.edu.ua/method/getfile.php?fname=132812.pdf&x=1 (дата звернення: 23.11.2023).
8. Савченко В.А., Шаповаленко О.Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. *Сучасний захист інформації*. 2020. № 4 (44). 6-11 с. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2456/2356 (дата звернення: 23.11.2023).
9. Global Risks Report 2022. *World Economic Forum* : веб-сайт. URL: https://www.weforum.org/publications/global-risks-report-2022/in-full/chapter-3-digital-dependencies-and-cyber-vulnerabilities/ (дата звернення: 23.11.2023).
10. Cybersecurity - Ukraine | Statista Market Forecast. *Statista* : веб-сайт. URL: https://www.statista.com/outlook/tmo/cybersecurity/ukraine (дата звернення: 23.11.2023).

Азарова Анжеліка Олексіївна – к.т.н., професор кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, azarova.angelika@gmail.com

Azarova A. Anzhelika – Ph.D., Professor, Department of Information Systems Management and Security, Vinnytsia National Technical University, Vinnytsia, e-mail: azarova.angelika@gmail.com

Смоляк Ігор Анатолійович — студент групи 1КІТС-22м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: igor14smolyak@gmail.com

Smolyak Igor A. – student of 1CITS-22m group, Faculty of management and information security, Vinnytsa National Technical University, Vinnytsia, e-mail: igor14smolyak@gmail.com