



ПРОГРАМНО-ТЕХНІЧНІ КОМПЛЕКСИ

УДК 519.7:65.011

А.О. АЗАРОВА

Вінницький національний технічний університет, Вінниця, Україна,
e-mail: azarova.angelika@gmail.com.

Ю.В. КРАК

Київський національний університет імені Тараса Шевченка, Київ, Україна,
e-mail: iurii.krak@knu.ua.

О.Г. МУРАЩЕНКО

Вінницький національний технічний університет, Вінниця, Україна,
e-mail: Oleksandr.Murashchenko@gmail.com.

Л.О. НІКІФОРОВА

Вінницький національний технічний університет, Вінниця, Україна,
e-mail: nikiforovalilia@gmail.com.

О.В. РУЗАКОВА

Вінницький державний педагогічний університет імені Михайла Коцюбинського,
Вінниця, Україна, e-mail: olgarkv81@gmail.com.

ОЦІНЮВАННЯ ВРАЗЛИВОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ ЗАСОБАМИ НЕЙРОМЕРЕЖІ ХЕММІНГА¹

Анотація. Опрацьовано наявний теоретичний доробок щодо оцінювання рівня захисту інформаційних систем (ІС) на основі різних підходів, зокрема використання нейронних мереж та штучного інтелекту. Це уможливило розроблення математичної та структурної моделей процесу оцінювання рівня інформаційної безпеки ІС та методу їхньої формалізації на основі системного підходу, нейронної мережі Хеммінга та елементів штучного інтелекту. Обґрунтовано множину оцінювальних параметрів рівня захищеності сучасних ІС та розроблено цифрову технологію для ідентифікації вразливостей у їх захисті засобами нейронної мережі Хеммінга та з використанням штучного інтелекту. Експериментальний пул верифікації розробленої моделі складають інформаційні системи десяти компаній.

Ключові слова: цифрова технологія, інформаційна безпека, вразливість інформаційних систем, нейронна мережа Хеммінга, штучний інтелект.

ВСТУП ТА ОГЛЯД ЛІТЕРАТУРИ

Інформаційна безпека (ІБ) є важливою частиною сучасного світу, де захист даних та інформації має критичне значення. Вона містить заходи для забезпечення конфіденційності, доступності та цілісності інформації. ІБ визначає багато видів загроз та має в арсеналі численні методи захисту, які залежать від сфери застосування, властивостей інформації, принципів дотримання безпеки, законодавчих вимог та інших чинників.

Стан ІБ визначається рівнем вразливості системи оброблення й зберігання даних, за якого забезпечено конфіденційність, доступність і цілісність інформації, або комплексом заходів, спрямованих на захист інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, запису чи знищення [1].

Вразливість інформаційної безпеки — це властивість інформаційної системи (ІС) або програмного забезпечення, яка створює потенційну можливість для

¹ Дослідження частково здійснено в рамках програми КПКВК 6541230 НАН України.

атаки або порушення її безпеки. Вразливості можуть виникати унаслідок помилок у програмному коді, недоліків у проектуванні системи, слабкостей у реалізації криптографічних алгоритмів, підозрілих конфігурацій, незадовільних мережевих налаштувань та інших технічних причин. Як зазначено в дослідженнях [1, 2], оцінювання вразливостей інформаційної безпеки є надзвичайно важливим у сучасному цифровому світі, де інформаційні технології впроваджуються в різних сферах життя, і кіберзагрози стають повсякденним явищем для багатьох організацій та індивідів. Зростання кіберзагроз та їхньої складності вимагає постійного аналізу вразливостей для виявлення нових загроз та забезпечення відповідного захисту. У роботі [2] зазначено, що ефективний захист інформаційних ресурсів в умовах цифровізації потребує впровадження інтелектуальних систем виявлення загроз, зокрема на основі штучного інтелекту (ШІ). Особлива увага приділяється спроби цілісності і конфіденційності критично важливих даних.

Розвиток інформаційних технологій у різних галузях людської діяльності створює нові можливості для атак і збільшує потенційний обсяг вразливостей, які потрібно визначати та зменшувати. Як стверджується у роботі [3], захист даних та інформаційних ресурсів стає ключовим завданням в умовах зростання важливості цих активів та зменшення лояльності до втрати конфіденційності [4] та цілісності інформації. У цьому контексті аналіз вразливостей є незамінним інструментом для підвищення рівня безпеки інформаційних систем і даних [5, 6].

Для належного реагування на вразливості інформаційної безпеки потрібно належним чином оцінювати ризики [7], тобто визначати слабкі місця в інформаційних системах, які можуть використовувати зловмисники для атаки, крадіжки або компрометації даних. На думку авторів [8–12], цей процес допомагає оцінити рівень ризику та вживати заходів для підвищення рівня безпеки і, зазвичай, базується на використанні різноманітних нейромереж.

Одним із інструментів для здійснення діяльності в сфері ІБ є використання ШІ. У роботах [13–15] доведено, що використання ШІ в ІБ зумовлює значне підвищення ефективності захисту від кіберзагроз завдяки автоматизації процесів виявлення, аналізу та реагування на потенційні загрози. ШІ дає змогу оперативно виявляти аномалії у мережевому трафіку та активації, розпізнавати нові види кібератак, ідентифікувати зразки шкідливого коду та здійснювати аналіз логфайлів. Усі ці процеси відбуваються в режимі реального часу, скорочуючи час реакції на загрози, а також зменшує потребу постійного контролю людини. Такий підхід сприяє покращенню загального рівня безпеки ІС та даних, запобігає атакам та мінімізує можливі збитки унаслідок кіберінцидентів [15].

Отже, на сьогодні існує значний теоретичний доробок, який уможливорює реалізацію процесів захисту інформації. Але слід зазначити, що не всі проблеми висвітлено в науковій літературі. Зокрема, недостатньо обґрунтовано множину чинників, що характеризують вразливості ІС, яка б відповідала критеріям повноти, мінімальності та дієвості, що дає змогу точно оцінювати всі чинники впливу на такий процес. Крім того, слабо формалізовано процес відображення такої множини вхідних параметрів на множину вихідних рішень. А це, своєю чергою, унеможливорює розроблення ефективних засобів підвищення ІБ, що зумовлює актуальність подальших досліджень у цьому напрямку авторами статті.

Однією з ключових характеристик ІБ є наявність вразливостей такої безпеки, що є слабким місцем в інформаційній системі, яке може бути використане різними особами (зловмисниками) для атаки, крадіжки або компрометації даних. Уразливості можуть бути пов'язані з апаратним забезпеченням, програмним забезпеченням, мережею, персоналом, сайтом або організацією. Для їхнього усунення потрібно здійснювати регулярні перевірки, виявляти та мінімізувати ризики, застосовуючи моніторинг стану системи та вживати відповідних заходів безпеки.

Основні завдання цього дослідження:

- аналіз наявних інструментів та методів оцінювання вразливостей інформаційної безпеки ІС;
- розроблення структурної та математичної моделей процесу оцінювання вразливості ІБ;
- побудова математичного методу оцінювання рівня вразливості ІС за допомогою нейронної мережі Хеммінга;
- розроблення технології оцінювання рівня вразливості сучасних ІС на базі запропонованих математичної моделі та методу.

Отже, у цій статті запропоновано підхід, який ґрунтується на аналізі інформаційних ризиків за допомогою нейронної мережі Хеммінга з використанням ШІ, що дає змогу ефективно оцінити рівень інформаційної безпеки на прикладі експериментального пулу ІС десяти компаній.

АНАЛІЗ СУЧАСНИХ ІНСТРУМЕНТІВ ТА МЕТОДІВ ОЦІНЮВАННЯ РІВНЯ ВРАЗЛИВОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІС

Аналіз методів оцінювання вразливості інформаційної безпеки є ключовим для надійного захисту цифрових ресурсів в умовах зростаючих кіберзагроз. Існують різні підходи до оцінювання, зокрема NIST SP800-30, CRAMM, OCTAVE, FRAP, EBIOS [16–22], які охоплюють як кількісні, так і якісні методи оцінювання. Розглянемо основні підходи до оцінювання вразливості інформаційної безпеки ІС. Методи, наведені в табл. 1, дають змогу виявляти вразливості, аналізувати ризики, планувати заходи безпеки та адаптуватися до змін середовища. Вибір методології залежить від потреб організації, її масштабу та вимог до гнучкості, глибини аналізу й автоматизації процесів.

Проаналізуємо популярні цифрові інструменти, які дають змогу оцінювати вразливості інформаційної безпеки ІС. Порівняльний аналіз основних із цих інструментів наведено в табл. 2.

Зазначимо, що нейромережа Хеммінга [28] є ефективним цифровим інструментом для автоматизованого виявлення вразливостей інформаційних систем, оскільки аналізує нормальну поведінку та фіксує найменші відхилення, що можуть свідчити про загрози. Використання методів машинного навчання уможливорює моніторинг безпеки в реальному часі та дає змогу своєчасно реагувати

Таблиця 1. Переваги та недоліки основних методів оцінювання вразливості інформаційної безпеки ІС

Метод оцінювання	Суть методу	Переваги	Недоліки
NIST SP800-30	Якісний аналіз загроз і вразливостей інформаційних активів із визначенням ризиків	Деталізований підхід, офіційний стандарт, адаптивність	Повільний процес, часткова автоматизація
CRAMM	Комплексна методологія з поєднанням баз знань і сценаріїв оцінювання ризиків	Гнучкість для різних типів ІС, модульність, інтеграція профілів	Потреба у спеціалізованому програмному забезпеченні, складність для новачків
OCTAVE	Стратегічний підхід до оцінювання вразливостей через аналіз активів, загроз та заходів	Орієнтація на внутрішній контекст організації, методичність	Великий обсяг роботи, потребує міждисциплінарності
FRAP	Спрощене якісне оцінювання найкритичніших систем і можливих впливів	Проста реалізація, фокус на бізнес-критичних ІС, швидкість	Обмежена глибина, відсутність детального технічного аналізу
EBIOS	Методологія якісного оцінювання ризиків за допомогою аналізу цілей безпеки	Структурованість, орієнтація на інформаційні системи, гнучкість для адаптації	Складна для впровадження без попереднього навчання, менш поширена за межами Європейського Союзу

Таблиця 2. Переваги та недоліки основних цифрових інструментів оцінювання вразливості [17, 18, 23–27]

Інструмент	Призначення	Тип аналізу	Переваги	Недоліки
Nessus	Сканування систем і мереж на низку відомих вразливостей	Автоматизоване сканування	Висока точність, велика база вразливостей, зручний GUI [23]	Комерційна ліцензія, потребує постійного оновлення
OpenVAS	Відкрита альтернатива Nessus для оцінювання вразливостей	Автоматизоване сканування	Безкоштовний, активна спільнота, розширюваність	Менш інтуїтивний інтерфейс, потребує конфігурації
Metasploit	Тестування на проникнення (експлуатація вразливостей)	Активний аналіз (penetration testing)	Потужний фреймворк, база готових експлойтів	Високий поріг входу, може бути небезпечним у разі неправильного використання
Wireshark	Аналіз мережевого трафіку в реальному часі	Пакетний / протокольний аналіз	Детальне вивчення протоколів, діагностика мережі	Не сканує вразливості напряму
Burp Suite	Тестування вебзастосунків на вразливості	Аналіз вебтрафіку і вразливостей	Зручний для аналізу XSS, SQLi [27] тощо, інтеграція з браузером	Безкоштовна версія обмежена, потребує знань з веббезпеки

на потенційні атаки, підвищуючи рівень захисту інформаційних ресурсів. Використання нейромережі Хеммінга для автоматизації оцінювання вразливості інформаційної безпеки є доцільним з таких причин:

- мережа ефективна у виявленні й виправленні помилок, що важливо для забезпечення цілісності даних;
- захищена від пошкоджень: здатна виявляти зміни, спричинені випадковими або зловмисними діями;
- розпізнає патерни: аналізує дані та виявляє аномалії, що може вказувати на вразливості захисту ІС;
- легко реалізується програмним кодом, що уможливорює швидке автоматизоване оцінювання ризиків захищеності ІС;
- може комбіновано застосовуватися, доповнюючи інші методи, що дає змогу підвищити загальний рівень захисту.

Завдяки цьому мережа Хеммінга є ефективним інструментом для виявлення й усунення вразливостей у системах безпеки сучасних ІС.

Інтегрування ШІ в запропонованій моделі зводиться до:

- 1) автоматичного аналізу логів для виявлення аномалій, що можуть свідчити про потенційні загрози;
- 2) використання нейромереж, що є ефективним для аналізу даних та прогнозування можливих векторів атак;
- 3) визначення найбільш критичних вразливостей, їхнє усунення з урахуванням пріоритету та пропозицій ефективних контрзаходів;
- 4) моделі ШІ дають змогу аналізувати поведінку користувачів і виявляти потенційні спроби соціальної інженерії.

Загалом із впровадженням ШІ ця модель стає ефективнішою та дає змогу не лише оцінювати рівень вразливостей, а й прогнозувати потенційні ризики безпеки ІС, автоматизувати їхнє усунення та покращувати загальну ІБ організації.

ШІ інтегровано у модель кількома ключовими параметрами, зокрема для виявлення загроз, керування оновленнями, соціальної інженерії та доступу.

МАТЕМАТИЧНА ТА СТРУКТУРНА МОДЕЛІ ПРОЦЕСУ ОЦІНЮВАННЯ РІВНЯ ВРАЗЛИВОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІС

Вразливість інформаційної безпеки ІС є комплексною категорією, визначення якої є систематичним і структурованим процесом, що зумовлює ідентифікацію,

аналіз та оцінювання потенційно слабких місць і ризиків. У межах цього процесу здійснюють перевірку програмного забезпечення, мережевої архітектури, налаштувань систем та політик безпеки з метою виявлення потенційних загроз та визначення їхніх наслідків для захищеності та конфіденційності даних. Така процедура полягає в аналізі ризиків та ймовірності їхнього виникнення, призначенні пріоритетів щодо виправлення або захисту вразливості, а також розробленні стратегій та планів для запобігання можливим загрозам.

Структурну модель (рис. 1) процесу оцінювання рівня вразливості ІБ з використанням нейромережі Хеммінга зобразимо послідовністю відображення множини вхідних оцінювальних параметрів на множину вихідних рішень.

Для побудови математичної моделі такого процесу позначимо множину вхідних оцінювальних параметрів як $X = \{x_i\}, i = 1, \dots, n$, а вихідних рішень як $Y = \{y_j\}, j = 1, \dots, m$. Така модель дає змогу відобразити множину X параметрів x_i вразливості ІБ досліджуваної ІС на множину Y вихідних рішень.

Математичну модель процесу оцінювання рівня захищеності ІС подаємо у вигляді відображення множини X^* первинних вхідних параметрів x_k^* на множину Y вихідних рішень, реалізуючи функціонали F_1 та F_2 :

$$X^* \xrightarrow{F_1} X \xrightarrow{F_2} Y, \quad X = F_1(X^*), \quad X^* = \{x_k^*\}, \quad k = 1, \dots, 40,$$

$$Y = F_2(X), \quad X = \{x_i\}, \quad i = 1, \dots, 10, \quad Y = \{y_j\}, \quad j = 1, \dots, 3.$$

Тут функціонал F_1 реалізує такі функції, що оцінюють вхідні параметри:

$$x_1 = f(x_1^*, \dots, x_7^*); \quad x_2 = f(x_8^*, \dots, x_{10}^*); \quad x_3 = f(x_{11}^*, \dots, x_{13}^*);$$

$$x_4 = f(x_{14}^*, \dots, x_{16}^*); \quad x_5 = f(x_{17}^*, \dots, x_{19}^*); \quad x_6 = f(x_{20}^*, \dots, x_{22}^*);$$

$$x_7 = f(x_{23}^*, \dots, x_{25}^*); \quad x_8 = f(x_{26}^*, \dots, x_{30}^*);$$

$$x_9 = f(x_{31}^*, \dots, x_{33}^*); \quad x_{10} = f(x_{34}^*, \dots, x_{40}^*).$$

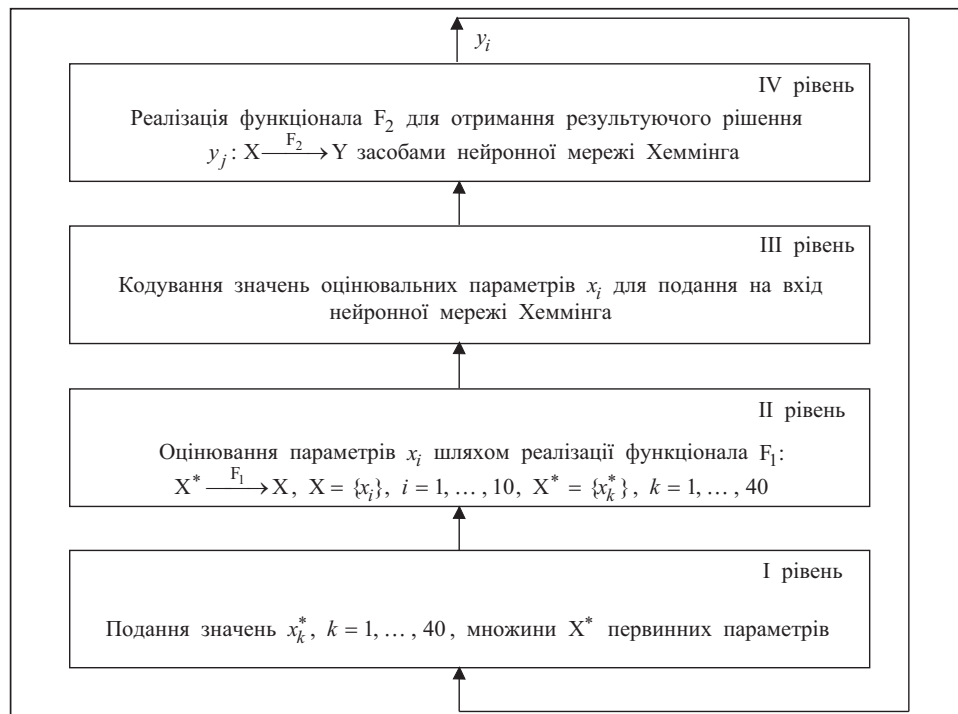


Рис. 1. Структурна модель процесу оцінювання рівня вразливості інформаційної безпеки ІС

Опишемо множину вхідних оцінювальних параметрів як вразливості: x_1 — автентифікації та авторизації в ІС; x_2 — захищеності вебзастосунку; x_3 — керування доступом до ІС; x_4 — шифрування даних в ІС; x_5 — мережевої безпеки; x_6 — фізичної безпеки ІС; x_7 — соціальної інженерії; x_8 — системи виявлення та запобігання вторгнень до ІС; x_9 — втрати даних ІС; x_{10} — оновлення ІС.

Множину вихідних рішень Y ідентифіковано такими рівнями вразливості інформаційної безпеки ІС: y_1 — низький рівень; y_2 — середній рівень; y_3 — високий рівень.

Зважаючи на специфіку оцінювальних параметрів x_i , запропоновано ідентифікувати їх з використанням лінгвістичних термів Н, С, В, де Н — низький рівень вираженості параметра x_i , С — середній, В — високий рівень вираженості параметра.

У табл. 3 наведено алгоритми ідентифікації лінгвістичних рівнів оцінювальних параметрів x_i як функцій від первинних вхідних параметрів x_k^* .

Таблиця 3. Алгоритм присвоєння значенню параметра x_i відповідного лінгвістичного терму

Оцінювальні параметри x_i	Первинні вхідні параметри x_k^*	Лінгвістичний терм, що описує значення оцінювального параметра x_i
1	2	3
x_1 — вразливості автентифікації та авторизації в ІС	x_1^* — використання слабких паролів обсягом до 7 символів	В
	x_2^* — відсутність ШІ-механізмів поведінкової автентифікації (тільки класичні паролі)	
	x_3^* — використання паролів із низькою ентропією, таких як «pass-word123» обсягом 7–9 символів	С
	x_4^* — використання паролів із високою ентропією обсягом від 9 до 12 символів і більше без Multi-Factor Authentication (MFA, багатофакторна автентифікація).	
	x_5^* — використання ШІ-аналізу активності користувачів (наприклад, виявлення аномальної поведінки) для контролю доступу	
	x_6^* — використання ІС паролів із високою ентропією (обсягом 9–12 символів і більше) з MFA	Н
	x_7^* — наявність в ІС ШІ-базованої поведінкової автентифікації (наприклад, динамічне оцінювання ризику сесій на основі поведінкових моделей)	
x_2 — вразливості захищеності вебзастосунку	x_8^* — відсутність механізмів безпеки вебзастосунку	В
	x_9^* — використання стандартних механізмів безпеки вебзастосунку: HTTPS, OWASP, CORS, CSP [17–20]	С
	x_{10}^* — використання передових технік (WAF, XSS) безпеки вебзастосунку [21, 27]	Н
x_3 — вразливості керування доступом до ІС	x_{11}^* — відсутність налаштувань рольового керування із обмеженням прав доступу (всі користувачі мають адміністративні привілеї)	В
	x_{12}^* — використання рольового керування для об'єднаної групи користувачів	С
	x_{13}^* — використання деталізованого рольового керування (застосування принципу найменших привілеїв)	Н

1	2	3
x_4 — вразливості шифрування даних в ІС	x_{14}^* — використання застарілих алгоритмів шифрування: DES, MD5, RSA, RC4 [17, 18, 21]	В
	x_{15}^* — використання стандартних алгоритмів шифрування (AES < 128 біт, RSA < 2048 біт) [19, 21]	С
	x_{16}^* — використання сучасних алгоритмів шифрування з великою довжиною та унікальністю ключів (AES $\geq$ 256 біт, RSA $\geq$ 3072 біт)	Н
x_5 — вразливості мережевої безпеки	x_{17}^* — відсутність брандмауерів	В
	x_{18}^* — використання брандмауерів для фільтрації та контролю трафіку типу WAF [17, 21]	С
	x_{19}^* — комплексне використання брандмауерів типу NGFW [29]	Н
x_6 — вразливості фізичної безпеки	x_{20}^* — відсутність контролю доступу до ІС	В
	x_{21}^* — застосування контрольованого доступу до ІС	С
	x_{22}^* — застосування системи доступу до ІС на базі біометричних показників	Н
x_7 — вразливості соціальної інженерії	x_{23}^* — відсутність проведення навчання персоналу з питань безпеки	В
	x_{24}^* — ситуативне проведення навчання персоналу з питань безпеки після інцидентів порушення ІБ	С
	x_{25}^* — постійне проведення навчання персоналу з питань безпеки засобами ШІ	Н
x_8 — вразливості системи виявлення та запобігання вторгнень до ІС	x_{26}^* — відсутність: систем виявлення вторгнень до ІС або використання ШІ-моделей у системах виявлення загроз	В
	x_{27}^* — використання звичайних систем виявлення вторгнень до ІС: IDS, IPS [30]	С
	x_{28}^* — використання стандартних AI-рішень для аналізу загроз, таких як прості ML-алгоритми в IDS / IPS [30]	Н
	x_{29}^* — використання ІС автоматичного реагування на загрози: SIEM, Palo Alto Networks Panorama [31]	
	x_{30}^* — виявлення загроз в ІС на базі ШІ (наприклад, SIEM з ШІ-аналітикою, Palo Alto Cortex XDR) [32]	
x_9 — вразливості втрати даних ІС	x_{31}^* — відсутність резервного копіювання даних	В
	x_{32}^* — резервне копіювання даних у ручному режимі	С
	x_{33}^* — автоматизоване резервне копіювання даних	Н
x_{10} — вразливості щодо оновлення ІС	x_{34}^* — використання застарілих версій (більше одного року) ІС	В
	x_{35}^* — відсутність використання ШІ для оцінювання безпеки оновлень ІС	
	x_{36}^* — несвоєчасне оновлення ІС або таке, що виконується вручну без чіткого регламенту	С
	x_{37}^* — автоматичне оновлення програмного забезпечення без перевірки на сумісність та безпеку	
	x_{38}^* — часткове використання ШІ для аналізу ризиків оновлень (наприклад, виявлення конфліктів оновлення)	
	x_{39}^* — автоматичне оновлення ІС із попереднім тестуванням у безпечному середовищі (sandbox)	Н
	x_{40}^* — автоматичне оновлення ІС із ШІ-аналізом стабільності та ризиків	

Зазначимо, що наведений перелік вразливостей з визначенням лінгвістичних термів оцінюваних параметрів сформовано з використанням джерела [33].

ПОБУДОВА МЕТОДУ ІДЕНТИФІКАЦІЇ ЛІНГВІСТИЧНИХ ПОКАЗНИКІВ РІВНЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІС НА ОСНОВІ НЕЙРОМЕРЕЖІ ХЕММІНГА

Для реалізації функціонала F_2 запропоновано використовувати нейронну мережу Хеммінга [28, 33]. Такий процес зводиться до відображення значень множини оцінювальних параметрів x_i , бінарні коди (мережа Хеммінга використовує лише 1 і -1) яких подаються на вхід нейромережі, на множину вихідних рішень $Y = \{y_j\}$, $j = 1, \dots, m$. Тоді для сигналу, поданого на її вхід (бінарного вектора значень оцінювальних параметрів x_i , що є функціями x_k^* (див. табл. 1)), вона знаходить відповідний еталонний зразок щодо рівня захищеності ІС. Це дає змогу приймати точне рішення, сприяючи надійному оцінюванню та керуванню вразливостями ІС.

Щоб отримати еталонні зразки для роботи нейромережі Хеммінга [28], застосовували експертний метод Делфі [34]. Для цього було запрошено фахівців з кібербезпеки і перевірено коефіцієнт конкордації отриманих колективних оцінок. У табл. 4 наведено сформовані експертами найтипівіші еталони для роботи мережі Хеммінга.

Нейромережа Хеммінга використовує тільки числові значення 1 та -1, тому потрібно закодувати три характеристичних терми: Н, С, В, що описують значення вхідних оцінювальних параметрів x_i та вихідних параметрів y_j , відповідним двійковим кодом. Закодуємо значення параметрів у мережі Хеммінга.

- Значення вхідних параметрів x_i : низький рівень -1, середній рівень -1, високий рівень 1.
- Значення вихідних параметрів y_j : низький рівень -1, середній рівень 1, високий рівень 1.

Представимо еталони, наведені у табл. 4, відповідними бінарними кодами для мережі Хеммінга (табл. 5).

Отже, мережа Хеммінга дає змогу порівняти поданий на її вхід вектор, що являє собою 20 закодованих значень десяти оцінювальних параметрів x_i вразливості ІБ ІС, із еталонними векторами (див. табл. 5) та ідентифікує той еталон,

Таблиця 4. Еталонні зразки для нейромережі Хеммінга

Номер еталона	Значення показників x_i та y_j										
	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	y_j
1	Н	Н	Н	Н	Н	Н	Н	Н	Н	Н	Н
2	Н	С	Н	Н	С	Н	Н	С	С	С	
3	С	С	С	С	С	С	С	С	С	С	С
4	С	В	В	С	В	В	В	С	С	С	В
5	В	В	В	В	В	В	В	В	В	В	

Таблиця 5. Коди еталонних зразків для мережі Хеммінга

Номер еталона	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	y_j
1	-1 -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	-1 1	
3	-1 1	-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	1 1
5	1 1	1 1	1 1	1 1	1 1	1 1	1 1	1 1	1 1	1 1	

що є найближчим до вектора, поданого на вхід. Номер такого еталона, який наведено у табл. 5, дає змогу класифікувати результативне рішення щодо рівня y_j (Н, С або В) вразливості інформаційної безпеки ІС.

Рівні реалізації функціоналів F_1 та F_2 запропонованої математичної моделі містять такі алгоритмічні рішення:

- подання значення x_k^* , $k = 1, \dots, 40$, первинних вхідних параметрів, що використовуються для розрахунку оцінювальних параметрів x_i , $i = 1, \dots, 10$, вразливості ІС;
- значення оцінювальних параметрів x_i , $i = 1, \dots, 10$, описуються конкретним лінгвістичним термом (Н — низький, С — середній, В — високий) шляхом реалізації функціонала F_1 згідно з табл. 3;
- для відображення функціонала F_2 формування вхідного вектора закодованих значень оцінювальних параметрів x_i (який складається з 20 цифр 1 та -1) для функціонування мережі Хеммінга та формування відповідних еталонних зразків;
- визначення нейромережею Хеммінга найближчого до поданого на вхід вектора еталона, номер якого відповідає певному вихідному рішенням y_j .

ЕКСПЕРИМЕНТАЛЬНА ЧАСТИНА

Для автоматизації запропонованої математичної моделі та методу її формалізації для ідентифікації рівня вразливості інформаційної безпеки ІС розроблено відповідну програму мовою С# і реалізовано на прикладі пулу з десяти вітчизняних ІС, зокрема ERP «Вправно» [35], ERP «Master» [36], «Своя CRM» [37], HRM «Hurta» [38] та ін. (табл. 6).

Для перевірки адекватності побудованої математичної моделі та методу її формалізації було порівняно результати, отримані за допомогою розробленої цифрової технології, із результатами для десяти вибраних для експерименту ІС з різних сфер застосування, одержаними з використанням традиційних інформаційних технологій (ІТ): Nessus, OpenVAS, Metasploit, Wireshark, Burp Suite [23–27] (табл. 7).

Порівняння оцінок рівнів вразливостей ІБ десяти сучасних ІС свідчить про коректність і адекватність розробленої у цій роботі технології. Зазначимо, що використання запропонованої технології, яка побудована на базі розроблених математичної моделі та методу її формалізації з використанням нейромережі Хеммінга, має такі переваги: забезпечення цілісності інформації; точність результатів; захист від помилок; використання та врахування значної кількості

Таблиця 6. Результат використання розробленої ІТ для оцінювання вразливостей інформаційної безпеки десяти вітчизняних ІС

Номер ІС	Значення показників x_i та y_j										Рівень вразливості y_j
	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	
1	С	В	В	С	В	В	В	Н	С	С	Високий
2	Н	С	В	С	С	С	С	С	С	С	Середній
3	Н	Н	Н	С	Н	Н	Н	С	Н	С	Низький
4	С	В	В	С	С	В	В	С	В	Н	Високий
5	Н	С	С	С	В	С	С	Н	С	С	Середній
6	С	В	С	С	В	С	В	Н	С	В	Високий
7	Н	С	В	С	С	В	С	В	С	С	Середній
8	С	Н	Н	Н	Н	С	Н	С	Н	Н	Низький
9	С	В	В	С	В	В	В	С	Н	В	Високий
10	С	Н	С	С	С	С	Н	С	С	С	Середній

Таблиця 7. Оцінки, отримані за запропонованою технологією та засобами програмного забезпечення Nessus, OpenVAS, Metasploit, Wireshark, Burp Suite

Номер компанії	Рівень вразливості u_j					
	за Nessus	за OpenVAS	за Metasploit	за Wireshark	за Burp Suite	за авторською технологією
1	В	С	В	В	В	В
2	С	С	С	Н	С	С
3	Н	Н	Н	С	Н	Н
4	В	В	С	В	В	В
5	С	С	В	С	С	С
6	В	С	В	В	В	В
7	С	С	Н	С	С	С
8	Н	Н	Н	С	Н	Н
9	В	В	В	В	С	В
10	С	С	В	С	С	С

оцінювальних параметрів; наявність елементів самостійного навчання; швидкість отримання результатів. Інтеграція елементів самонавчання дає змогу системі адаптуватися до нових умов та ідентифікувати нові загрози. При цьому швидкість видачі результатів забезпечує оперативність у реагуванні на потенційні ризики та впровадженні відповідних заходів безпеки.

ПРАКТИЧНА РЕАЛІЗАЦІЯ РОЗРОБЛЕНОЇ ІТ ДЛЯ ОЦІНЮВАННЯ ВРАЗЛИВОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІС

Згідно з метою цього дослідження на основі розробленої математичної моделі оцінювання вразливості інформаційної безпеки ІС було створено цифровий інструмент, що автоматизує такий процес засобами нейромережі Хеммінга.

Для написання такого вебсервісу використано платформу ASP.NET Core 3.1, мову програмування C# (backend), фреймворк Angular та мову програмування JavaScript (frontend). Розроблена технологія є інструментом для оцінювання вразливостей інформаційної безпеки ІС за допомогою нейронної мережі Хеммінга. Вона дає змогу вдосконалити, автоматизувати та прискорити процес оцінювання вразливостей інформаційної безпеки ІС на базі обґрунтованої за критеріями повноти, мінімальності та дієвості множини оцінювальних параметрів.

ВИСНОВКИ

Застосування розробленої технології дає змогу системно реалізувати процес ідентифікації рівня ризиків у критичних компонентах інформаційної безпеки ІС. Основні переваги такої технології:

- структурований підхід — математична модель охоплює всі основні аспекти безпеки: доступ, мережі, шифрування, оновлення, соціальні фактори та управління загрозами;
- гнучкість — можна адаптувати параметри та пороги оцінювання під конкретні організації або галузі;
- аналітичний потенціал — модель дає можливість не тільки оцінювати вразливості, а й будувати прогнози щодо їхнього впливу на безпеку системи.

Використання розробленої моделі дасть змогу підприємствам та організаціям оцінювати рівень ризиків інформаційної безпеки ІС і впроваджувати відповідну політику їх мінімізації або усунення. Для банків та фінансових установ завдяки цій ІТ стає можливим контроль безпеки транзакцій і захист даних клієнтів. Для складових критичної інфраструктури, таких як енергетика, транспортні системи,

телекомунікації тощо, можна використовувати запропоновану модель для оцінювання ризиків кіберзагроз. Також її можна застосовувати і як інструмент для кібербезпечових аудитів, що дає змогу швидко ідентифікувати слабкі місця ІС.

Перспективним напрямком подальших наукових пошуків є інтеграція розробленої ІТ з SIEM-системами та інструментами моніторингу мережевої безпеки; динамічне оновлення моделі — адаптація під нові загрози, алгоритми атаки та вразливості; розширення оцінювання на рівень загроз IoT та промислових систем з урахуванням специфічних ризиків для розумних пристроїв і автоматизованих систем, а також розроблення та впровадження окремих механізмів, які не просто оцінюють ризики, а й рекомендують конкретні дії для їхнього усунення або мінімізації.

СПИСОК ЛІТЕРАТУРИ

1. Khilenko V., Akhmetov B., Berdibayev R. et al. Increasing the speed of banking cybersecurity systems based on intelligent data analysis and artificial intelligence algorithms for predicting cyberattacks. *I. Cybernetics and Systems Analysis*. 2023. Vol. 59, N 4. P. 519–525. <https://doi.org/10.1007/s10559-023-00587-x>.
2. Alfaadhel A., Almomani I., Ahmed M. Risk-based cybersecurity compliance assessment system (RC2AS). *Applied Sciences*. 2023. Vol. 13, N 10. Article number 6145. <https://doi.org/10.3390/app13106145>.
3. Zhang D., Chen J., He Y., Lan X., Chen X., Dong C., Li J. A chunked and disordered data privacy protection algorithm: Application to resource platform systems. *Applied Sciences*. 2023. Vol. 13, N 10. Article number 6017. <https://doi.org/10.3390/app13106017>.
4. Azarova A.O., Krak I.V., Nikiforova L.O., Belyakova K.S. Applying systems analysis and mathematical apparatus of fuzzy logic to model the process of evaluating the financial state of the enterprise. *Cybernetics and Systems Analysis*. 2024. Vol. 60, N 6. P. 978–990. <https://doi.org/10.1007/s10559-024-00734-y>.
5. Azarova A., Azarova L., Krak I., Ruzakova O., Azarova V. Information system for assessing the level of human capital management. *Informatyka Automatyka Pomiary w Gospodarce i Ochronie Środowiska*. 2024. Vol. 14, N 3. P. 123–128. <https://doi.org/10.35784/iapgos.6159>.
6. Mashima D., Chen Y., Roomi M., Lakshminarayana S., Chen D. Cybersecurity for modern smart grid against emerging threats. *Foundations and Trends® in Privacy and Security*. 2023. Vol. 5, N 4. P. 189–285. <http://dx.doi.org/10.1561/33000000035>.
7. Azarova A., Azarova L., Nikiforova L., Azarova V., Teplova O., Kryvinska N. Neural network technologies of investment risk estimation taking into account the legislative aspect. *CEUR Workshop Proceedings*. 2020. Vol. 2805. P. 308–323. URL: <https://ceur-ws.org/Vol-2805/paper23.pdf>.
8. Azarova A., Azarova L., Pavlov S., Savina N., Kaplun I., Wójcik W., Smailova S., Kalizhanova A. Information technologies for assessing the quality of IT-specialties graduates' training of university by means of fuzzy logic and neural networks. *International Journal of Electronics and Telecommunications*. 2020. Vol. 66, N 3. P. 411–416. <https://doi.org/10.24425/ijet.2020.131893>.
9. Zhenxiang H., Zhenyu Z., Ke C., Yanlin L. Smart contract vulnerability detection method based on feature graph and multiple attention mechanisms. *Computers, Materials & Continua*. 2024. Vol. 79, N 2. P. 3023–3045. <https://doi.org/10.32604/cmc.2024.050281>.
10. Letychevskiy O. Cognitive networks, their properties and applications in attack detection and prevention systems. *Cybernetics and Systems Analysis*. 2023. Vol. 59, N 5. P. 859–866. <https://doi.org/10.1007/s10559-023-00621-y>.
11. Dubin R. Disarming attacks inside neural network models. *IEEE Access*. 2023. Vol. 11. P. 124295–124303. <https://doi.org/10.1109/ACCESS.2023.3330141>.

12. Wu H., Dong H., He Y., Duan Q. Smart contract vulnerability detection based on hybrid attention mechanism model. *Applied Sciences*. 2023. Vol. 13, N 2. Article number 770. <https://doi.org/10.3390/app13020770>.
13. Wen S.-F., Shukla A., Katt B. Artificial intelligence for system security assurance: A systematic literature review. *International Journal of Information Security*. 2025. Vol. 24, Iss. 1. <https://doi.org/10.1007/s10207-024-00959-0>.
14. Nitaj A., Rachidi T. Applications of neural network-based AI in cryptography. *Cryptography*. 2023. Vol. 7, N 3. Article number 39. <https://doi.org/10.3390/cryptography7030039>.
15. Berghoff C., Neu M., Twickel A. Vulnerabilities of connectionist AI applications: Evaluation and defense. *Front. Big Data*. 2020. Vol. 3. Article number 23. <https://doi.org/10.3389/fdata.2020.00023>.
16. Cybersecurity — Ukraine | Statista market forecast. Statista. URL: <https://www.statista.com/outlook/tmo/cybersecurity/ukraine>.
17. Alam S. Cybersecurity: Past, present and future. LAP LAMBERT Academic Publishing, 2022. 123 p.
18. Hashim N.A., Abidin Z.Z., Zakaria N.A., Puvanasvaran A.P., Ahmad R. Risk assessment method for insider threats in cyber security. *International Journal of Advanced Computer Science and Applications*. 2018. Vol. 9, N 11. P. 126–130. <https://dx.doi.org/10.14569/IJACSA.2018.091119>.
19. Shyian A.A., Nikiforova L.O. Ensuring information security and cybersecurity in the modern information space: models and methods. Vinnytsia: VNTU, 2024. 135 p.
20. Kuzminykh I., Ghita B., Sokolov V., Bakhshi T. Information security risk assessment. *Encyclopedia*. 2021. Vol. 1, N 3. P. 602–617. <https://doi.org/10.3390/encyclopedia1030050>.
21. Yevseiev S., Khokhlachova Yu., Ostapov S. et al. Models of socio-cyber-physical systems security. Kharkiv: PC TECHNOLOGY CENTER, 2023. 168 p. <https://doi.org/10.15587/978-617-7319-72-5>.
22. EBIOS Risk Manager. 2024. 100 p. URL: https://cyber.gouv.fr/sites/default/files/document/20240326_np_anssi_guide_ebios_fr_final_web.pdf (in French).
23. Pandit P. Nessus: Study of a tool to assess network vulnerabilities. 2021. <http://doi.org/10.13140/RG.2.2.14758.65604>.
24. Nisha P. Vulnerability scanning with OpenVAS: Unveiling cybersecurity insights. 2023. URL: <https://eunishap.medium.com/vulnerability-scanning-with-openvas-unveiling-cybersecurity-insights-eff56de79276>.
25. Raj S., Walia N.K. A study on metasploit framework: A pen-testing tool. *International Conference on Computational Performance Evaluation (ComPE)*. 2020. P. 296–302. <http://doi.org/10.1109/ComPE49325.2020.9200028>.
26. Soepeno R. Wireshark: An effective tool for network analysis. 2023. <http://doi.org/10.13140/RG.2.2.34444.69769>.
27. Introduction to Burp Suite, the tool dedicated to web application security. January 15, 2024 URL: <https://www.vaadata.com/blog/introduction-to-burp-suite-the-tool-dedicated-to-web-application-security/>.
28. Mezher L.S. Hamming neural network application with FPGA device. *International Journal of Reconfigurable and Embedded Systems (IJRES)*. 2021. Vol. 10, N 1. P. 37–46. <http://doi.org/10.11591/ijres.v10.i1.pp37-46>.
29. Next-generation firewall overview. URL: <https://www.cisco.com/site/NGFW>.
30. IDS/IPS. Cisco. URL: <https://search.cisco.com/IDS/IPS>.
31. What is the role of AI and ML in modern SIEM solutions? URL: https://www.paloaltonetworks.com/cyberpedia/role-of-artificial-intelligence-ai-and-machine-learning-ml-in-siem?utm_source=chatgpt.com.

32. CORTEX XDR URL: https://www.paloaltonetworks.com/cortex/cortex-xdr?utm_source=chatgpt.com.
33. Азарова А.О., Смоляк І.А. Інформаційна технологія для оцінювання вразливостей інформаційної безпеки сучасних ІС. *Тези Міжнародної науково-практичної Інтернет-конференції студентів, аспірантів та молодих науковців «Молодь в науці: дослідження, проблеми, перспективи»*. Вінниця: ВНТУ, 2024. URL: <https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/view/19660/16275>.
34. Sablatzky T. The delphi method. *Hypothesis: Research Journal for Health Information Professionals*. 2022. Vol. 34, N 1. <https://doi.org/10.18060/26224>.
35. ERP «Вправно». URL: <https://vpravno.com.ua/uk/>.
36. ERP «Master». URL: <https://masterbuh.com/>.
37. «Своя CRM». URL: <https://svoya.in.ua/>.
38. HRM «Hurma». URL: <https://hurma.work/>.

**A.O. Azarova, Iu.V. Krak, O.G. Murashchenko,
L.O. Nikiforova, O.V. Ruzakova**

**INFORMATION SYSTEM VULNERABILITY ASSESSMENT
USING HAMMING NEURAL NETWORK**

Abstract. The article reviews existing theoretical developments in the field of assessing the security level of information systems based on various approaches including the use of neural networks and artificial intelligence. This enabled the authors of the article to develop their own mathematical and structural models of the process of assessing the level of information security of IS and the method of their formalization based on a systems approach, a Hamming neural network and elements of artificial intelligence. A set of evaluation parameters of the level of security of modern IS was substantiated and a digital technology was developed for identifying vulnerabilities in IS security from various fields of application using a Hamming neural network and artificial intelligence. The experimental verification pool of the developed model consists of information systems of 10 companies.

Keywords: digital technology, information security, vulnerability of information systems, Hamming neural network, artificial intelligence.

Надійшла до редакції 15.06.2025