РОЗДІЛ ІІ. ІНФОРМАЦІЙНО-КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ

DOI: 10.25140/2411-5363-2021-3(25)-125-137
УДК 004.41.657

Валерій Лахно[1], Андрій Блозва[2], Єгор Часновський[3], Олена Криворучко[4], Альона Десятко[5]

[1]доктор технічних наук, професор, професор кафедри комп'ютерних систем та мереж
Національний університет біоресурсів та природокористування України (Київ, Україна)
E-mail: valss21@ukr.net. **ORCID:** http://orcid.org/0000-0001-9695-4543

[2]кандидат педагогічних наук, доцент, доцент кафедри комп'ютерних систем та мереж
Національний університет біоресурсів та природокористування України (Київ, Україна)
E-mail: andriy.blozva@nubip.edu.ua. **ORCID:** http://orcid.org/0000-0002-4377-0916

[3]аспірант кафедри комп'ютерних систем та мереж
Національний університет біоресурсів та природокористування України (Київ, Україна)
E-mail: egor.chasnovskii@gmail.com. **ORCID:** https://orcid.org/0000-0002-6360-4640

[4]доктор технічних наук, професор, завідувач кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет (Київ, Україна)
E-mail: ev_kryvoruchko@ukr.net. **ORCID:** http://orcid.org//0000-0002-7661-9227

[5]доктор філософії за спеціальністю комп'ютерні науки,
доцент кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет (Київ, Україна)
E-mail: desyatko@knute.edu.ua. **ORCID:** https://orcid.org/0000-0002-2284-3218

АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ ЗАСТОСУВАННЯ НЕЙРО-НЕЧІТКОЇ СИСТЕМИ

У статті запропоновано заходи щодо вдосконалення процедур аудиту інформаційної безпеки (АІБ) для різних об'єктів інформатизації (ОБІ). Показано, що оцінку рівня ступеня інформаційної безпеки (ІБ) для ОБІ доцільно проводити на основі оцінювання результативності безлічі критеріїв методу аналізу ієрархій (МАІ). При цьому така оцінка ступеня ІБ і всі пов'язані з нею процедури аудиту АІБ, найбільш ефективні для багатостороннього оцінювання ІБ ОБІ. Запропоновано модифікований метод аналізу ієрархій, на основі застосування апарату теорії нечітких множин і нейронних мереж. Цей метод дає можливість менеджменту приймати обґрунтовані управлінські рішення у сфері ІБ ОБІ.

Ключові слова: *аудит інформаційної безпеки; об'єкт інформатизації; метод аналізу ієрархій; інтелектуальна інформаційна система; нейронна мереж; нечітка логіка.*

Рис.: 4. Табл.: 1. Бібл.: 24.

Актуальність теми дослідження. Динаміка збільшення кількості та складності кібератак на різні об'єкти інформатизації (ОБІ) тільки за останні кілька років [1; 2] показує, що, незважаючи на всі зусилля з боку захисту протиставити атакуючим дедалі більше технічно досконалі апаратно-програмні засоби інформаційної безпеки (ІБ) і донині не втрачає актуальності проблема отримання поточних і прогнозних оцінок рівня ІБ ОБІ. Це завдання особливо стало актуальним для об'єктів критично важливої інфраструктури (КВІС) держави [3]. Адже несанкціоноване втручання в комп'ютерні системи (КС) може викликати збої в бізнес-процесах і відбитися на безпеці людей. Наприклад, навіть короткочасна відмова КС, зокрема, підприємств комунальної сфери, здатна викликати перебої в постачаннях електроенергії, води, перебої з постачанням у торговельних мережах і т. ін.

Чим складніша структура ОБІ і чим більш складними є інформаційні технології (ІТ) тим складніше побудувати для них систему управління їх інформаційною безпекою (СУІБ), яка відповідає сучасним вимогам. Безліч важливих об'єкт інформатизації апріорі потребує мати сучасну систему управління, зокрема, у питаннях, що стосуються ІБ. Подібного типу системи сьогодні стали невід'ємною частиною систем менеджменту (СМ). Відповідно, інтеграція подібних СМ у завдання забезпечення ІБ ОБІ передбачає необхідність побудови системи проведення періодичного аудиту ступеня захищеності ОБІ. Це, зокрема, можливо шляхом експертного або комп'ютерного отримання оцінок (метрик) ІБ у СУІБ.

Для того щоб побудувати ефективну СУІБ, необхідно дотримуватися такого алгоритму дій:

- по-перше, проєктування СУІБ ОБІ має виконуватися на основі ризик-орієнтованих стандартів;

- по-друге, формування вимог до бізнес-процесів ОБІ з погляду забезпечення ІБ, має виконуватися на основі використання чітких вимірних метрик ІБ;

- по-третє, завдання аудиту ІБ ОБІ повинно розглядатися комплексно, і в такій постановці цього завдання без комп'ютерної підтримки прийняття рішень обійтися складно.

Все вищевикладене зумовлює необхідність проведення нових досліджень у завданнях підвищення ефективності процедур аудиту інформаційної безпеки (АІБ) на основі комплексного застосування інтелектуальних систем.

Постановка проблеми. Наукову проблему цього дослідження можна сформулювати таким чином: «необхідно подолати суперечності між станом теорії інформаційної безпеки, в тій частині, яка регламентує вимоги до проведення аудитів ІБ ОБІ і залежними від траєкторії кіберзагроз сформованими практиками забезпечення ІБ ОБІ». Рішення зазначеної проблеми, зокрема, передбачає необхідність перегляду існуючих статичних моделей управління ІБ. Слід наголосити на одній із підзадач як необхідність вдосконалення системи АІБ. Отже, процедура прийняття рішень особою, яка приймає рішення при фіксованому переліку альтернатив, передбачає необхідність створення нових підходів до процедур аудиту ІБ.

Аналіз останніх досліджень і публікацій. Проблемі проведення аудиту ІБ для різних ОБІ присвячено досить багато робіт, з-поміж необхідно згадати ті, що стали класичним роботи для вирішення завдань АУІ [4; 5].

У роботі [6] показана важливість аналізу інформаційних потоків для коректного проведення процедур аудиту в інформаційних системах ОБІ. Але автор не розглядає потенціал застосування інтелектуальних систем для підвищення якості процедур аудиту ІБ.

У роботі [7] проведено аналіз взаємозв'язку процедур внутрішнього аудиту ІБ і зовнішнього аудиту. Однак авторами не взято до уваги постійний розвиток систем захисту ІБ. Зауважимо, що впровадження в контури ІБ новітніх систем ІБ, здатне змінити перелік базових метрик ІБ, прийнятих в організації.

У [8] аналізуються особливості проведення аудиту ІБ для погроз «нульового дня» (zero-day). Зокрема, авторами відзначено, що постачальники засобів ІБ зазвичай можуть запропонувати лише варіант постійного розвитку та вдосконалення технічних засобів захисту інформації (ЗЗІ).

У [9; 10] авторами також відслідковано, що, хоча постійне вдосконалення ЗЗІ необхідно, однак це «вигідно» переважно виробникам ЗЗІ. І лише одне вдосконалення ЗЗІ не здатна самостійно вирішити проблему постійного протистояння ЗЗІ і загроз ІБ. Однак, як показано в [11; 12], якщо сторона захисту стикається з цільовою (таргетованою) атакою, то покладатися лише на ЗЗІ буде помилкою.

У зв'язку з цим багатьма експертами [8; 13; 14] наголошується на необхідності застосування не лише технічних підходів (використання ЗЗІ) для протидії кібернетичним загрозам, але і впровадження комбінованих методів. Авторами детально не розкрито поняття комбінованих методів, але згадується необхідність їх побудови на базі сімейства стандартів ISO серії 27001 і 19011 [15-19].

Відзначимо, що методологія проведення аудиту ІБ добре відома й відпрацьована фахівцями, але поки не до кінця відпрацьованими є питання, що стосуються впровадження в процедури аудиту інтелектуальних систем підтримки прийняття рішень (ІСППР). При цьому зростаючі вимоги до якості проведення процедур аудиту ІБ диктують необхідність задіяння потенціалу ІСППР у ході оперативного реагування на виявлені загрози в інформаційних системах (ІС). А це робить завдання підвищення ступеня захищеності, а також отримання поточних і прогнозних оцінок ІБ ОБІ релевантним.

Виділення недосліджених частин загальної проблеми. У дослідженнях та публікаціях, які розглядались, не було виявлено потенціал застосування інтелектуальних систем для підвищення якості процедур аудиту ІБ та не прийнято до уваги постійний розвиток систем захисту ІБ; питання можливості зміни переліку базових метрик ІБ, прийнятих в організації, при впровадженні в контури ІБ новітніх систем ІБ; також оглянутій за тематикою літературі детально не розкриті поняття комбінованих методів, хоч згадується необхідність їх побудови на базі сімейства стандартів ISO серії 27001 і 19011 [15-19].

Постановка завдання. При вирішення завдання підвищення ступеня захищеності, а також отримання поточної та прогнозної оцінки ІБ ОБІ доцільно застосовувати точні чисельні оцінки – метрики ІБ [4; 5].

Цей вектор дослідження узгоджується з основними положеннями «базового» стандарту системи управління інформаційною безпекою 27004: 2009 [5]. Як джерела даних у ході реалізації процедур аудиту ІБ (як внутрішнього, так і зовнішнього) можуть бути використані такі відомості [6]:

- результати аналізу та оцінки ризиків для ІБ ОБІ;
- звіти попередніх процедур АІБ;
- журнали реєстрації інцидентів ІБ
- звіти систем виявлення вторгнень або/і такої категорії ПО, як Security information and event management (SIEM);
- повідомлення персоналу про інциденти ІБ;
- результати, отримані в ході тестування функціональних підсистем КС ОБІ;
- результати, отримані в ході тренінгів по ІБ персоналу ОБІ;
- та ін.

Таким чином, очевидна постановка завдань дослідження:

- розвиток методу СУІБ для проведення аудиту ІБ ОБІ й отримання чисельних поточних і/або прогнозних оцінок ступеня його захищеності в умовах динамічного протистояння з атакуючої стороною;
- розробка та апробація інтелектуальної системи підтримки прийняття рішень, спрямованих на збільшення ступеня ІБ з можливістю синтезу чисельної оцінки результативності аудиту ІБ ОБІ.

Викладення основного матеріалу.

Методи та моделі.

При розробці програми проведення аудиту ІБ (далі ПАІБ) не всі співвідношення між зв’язками АІБ, можуть враховуватися в конкретній ситуації. Це насамперед зумовлено відсутністю необхідної інформації.

При проведенні аудиту ІБ великих компаній або підприємств об’єкт аудиту цілком розглянути повною мірою досить складно. Аудиторам доцільніше вибрати найбільш важливі інформативні свідчення аудиту (далі СА) або метрики ІБ. Відібрані метрики і СА матимуть більшу значущість і при цьому вартість їх отримання буде невисока.

Зазвичай для того щоб побудувати модель об’єкта АІБ (далі ОАІБ), доцільно задіяти вагові коефіцієнти значущості доказів аудиту.

Як показала реальна практика проведення аудитів ІБ, облік значущості СА є складним завданням. При цьому важливим фактором є досвід аудитора і передусім особи, що відповідає за складання програми АІБ і системний аналіз одержуваних у процесі аудиту результатів. Не коректна постановка вихідних завдань АІБ може звести до нуля головну мету проведеного АІБ ОБІ або дати недостовірні результати. Усе вищезазначене обумовлює ефективність комбінації експертних і математичних методів обробки отриманих експертних оцінок. Як показав аналіз літературних джерел [10; 20], для вирішення зазначених вище завдань можуть застосовуватися методи парних порівнянь; бальних оцінок; векторів переваг; аналізу ієрархій (МАІ) та ін. Досить докладний аналіз результативності застосування цих методів представлений у [20].

Враховуючи, що відбір метрик ІБ для кожного ОБІ має свої особливості, які зумовлені викликами галузі ОБІ, так і ступенем його критичності. Саме це далі формалізує типову задачу відбору метрик АІБ. При цьому пропонується керуватися таким алгоритмом (рис. 1).

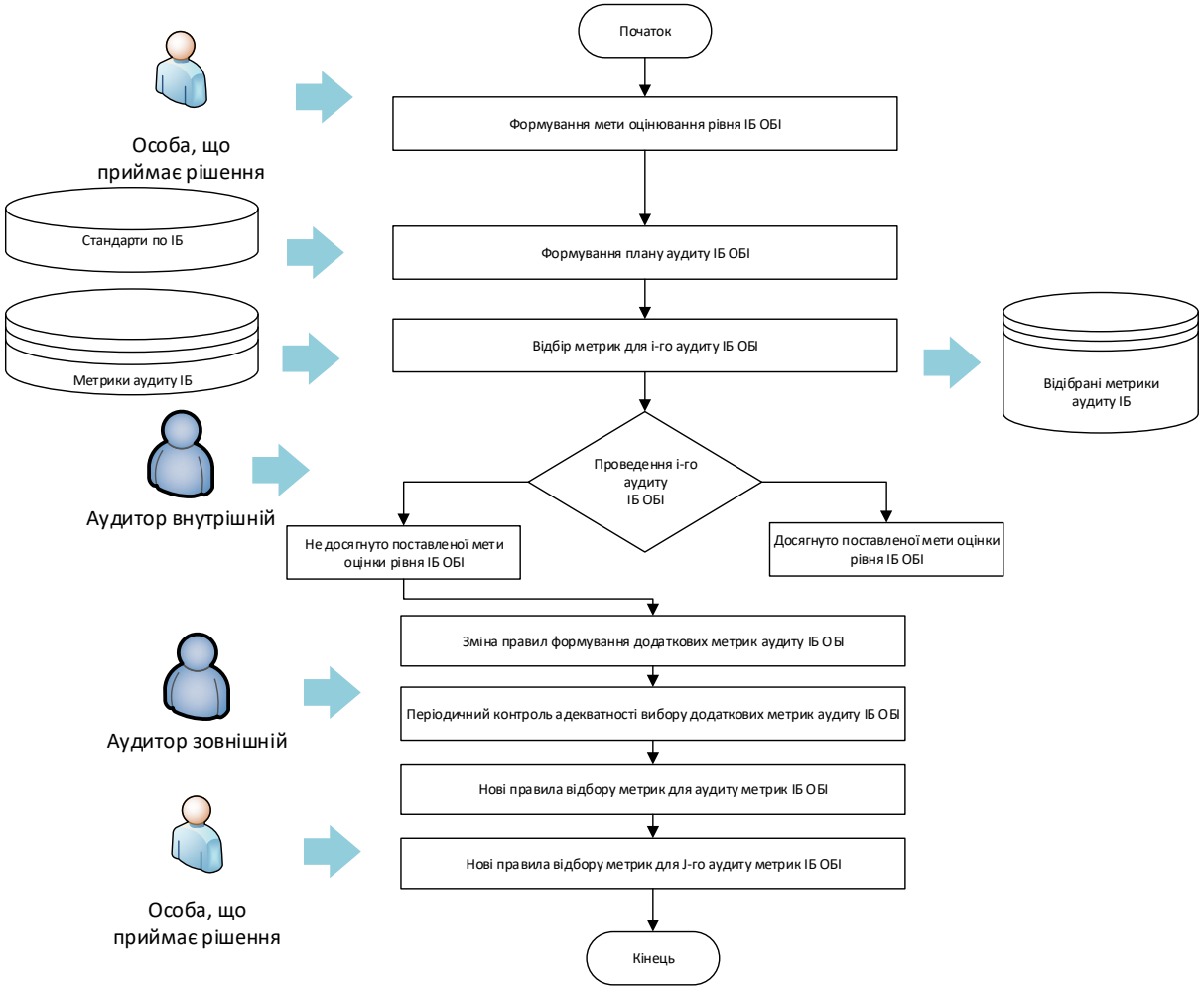


Рис. 1. Блок-схема алгоритму відбору індивідуальних критеріїв (метрик ІБ)

У модифікованому алгоритмі проведення аудиту ІБ, в порівнянні з базовими процедурами, необхідно брати до уваги такі нові обставини:

1. Слід орієнтуватися насамперед на відібрані аудиторами пріоритетні метрики ІБ. Ці відібрані аудиторами метрики могли раніше не зустрічатися протягом попереднього циклу процедури аудиту ІБ ОБІ;

2. Слід контролювати відхилення, що з'явилися, в якісних характеристиках відібраної метрики ІБ.

3. Слід формувати правила відбору і заміни раніше відібраних метрик ІБ, наприклад, керуючись результатами попередніх аудитів ІБ, або у зв'язку зі зміною траєкторії загроз для інформаційних систем ОБІ.

Побудова ієрархії метрик ІБ у ході аудиту така:

Етап 1. Визначаємо підцілі АІБ. Це можуть бути приватні задачі, наприклад:

- Оцінити доступність, конфіденційність, цілісність інформації в ІС.
- Обґрунтувати безлічі СА, які включені в програму АІБ (ПАІБ).
- Вивести відповідні аудиторські докази, які передбачені ПАІБ. Свідоцтва АІБ здебільшого розраховані аналітиками ІБ.

Етап 2. Відбираємо чинники, які важливі для 2-го рівня ієрархії ПАІБ.

- на цьому етапі збирають об'єктивні свідчення АІБ. До таких можна, наприклад, віднести, важливі з погляду критеріїв аудиту факти;
- фокусують сили і засоби АІБ. Наприклад, сюди відносяться аудиторські групи, окремі аудитори ІБ та ін.

Побудова ієрархії метрик ІБ під час ході аудиту наступна:

Етап 1. Визначаємо підцілі АІБ. Це можуть бути приватні задачі, наприклад:

- оцінити доступність, конфіденційність, цілісність інформації в ІС;
- обґрунтувати безлічі СА, які включені в програму АІБ (ПАІБ);
- вивести відповідні аудиторські докази, які передбачені ПАІБ. Свідоцтва АІБ як правило розраховані аналітиками ІБ.

Етап 2. Відбираємо чинники, які важливі для 2-го рівня ієрархії ПАІБ. На цьому етапі:

- збирають об’єктивні свідчення АІБ. До таких можна, наприклад, віднести, важливі з точки зору критеріїв аудиту факти;
- фокусують сили і засоби АІБ. Наприклад, сюди відносяться аудиторські групи, окремі аудитори ІБ та ін.

Зауважимо, що для кожного ОБІ завдання аудиту ІБ має свою специфіку, яка визначається ступенем критичності інформаційних процесів у бізнес-процесах організації.

З урахуванням публікацій [23] модифікувати БАІ за рахунок додаткового застосування таких кроків:

Крок 1. Оцінюємо стійкість локальних ранжувань на основі векторів змін в елементах матриць парних порівнянь.

Крок 2. Знаходимо експертні оцінки парних порівнянь, які найбільшою мірою впливають на зміну локальних ранжувань альтернатив рішень і зміна рівнів узгодженості безлічі оцінок.

Крок 3. Оцінюємо чутливість глобального ранжування альтернатив рішень до зміни ваги елементів ієрархії.

Крок 4. Знаходимо найбільш чутливі і стійкі елементи для кожного рівня ієрархії.

Фактично МАІ необхідний на етапі розрахунку проміжних показників, і визначення остаточного рангу об’єктів. Це аналогічно процедурам завдання функцій приналежності нечітких множин, що використовуються для опису об'єктів спостереження і вимог до них.

У МАІ для того щоб знайти ранг об’єкта застосовують формулу:

$$p_i = \sum_{j=1}^{n} g_j \cdot v_{ij}, \tag{1}$$

де $n-$ кількість критеріїв (метрик ІБ); g_j – показник важливості критерію (метрики ІБ); v_{ij} – показник переваги $i-$го об'єкта по $j-$му критерію.

Нескладно помітити певну схожість із найпростішою моделлю односпрямованої нейронної мережі. У теорії нейронних мереж для цього застосовують таку формулу [24]:

$$y = f\left(\sum_{i=0}^{N} w_i \cdot u_i\right), \tag{2}$$

де $N-$ кількість входів нейрона; w_0 – порогове значення; $u_0 = -1, \quad u_i -$ вхідний сигнал $i-$го нейрона; w_i – синаптичні ваги входів; $y-$ вихідний сигнал нейрона.

Очевидна схожість вищенаведених формул. У цьому випадку показник переваги об'єкта з різних метрик ІБ вимогам ставиться у відповідність до синаптичних ваг входів нейрона. Тоді процес обчислення параметрів переваг об’єкта за різними вимогами виконує функції навчання нейронів.

З огляду на специфіку завдання проведення аудиту ІБ, пропонуються такі зміни для модифікації БАІ. Це дозволяє не тільки врахувати специфіку предметної області проведення АІБ ОБІ, а й подальшої адаптації пропонованих змін для практичної реалізації інтелектуальної СППР з використанням методів об'єктноорієнтованого проєктування.

По-перше, введемо обмеження на вихідні дані. Це обумовлено особливостями організації процедури АІБ ОБІ. Безліч критеріїв оцінки ступеня кібербезпеки ОБІ, розділимо на дві частини. Це, відповідно, загальні та індивідуальні критерії (метрики ІБ).

Загальні критерії – це критерії, які ставляться до будь-яких ОБІ при проведенні АІБ. Ця множина не залежить від призначення і функціоналу, які реалізовані інформаційними системами ОБІ. Вважаємо, що безліч загальних критеріїв, наприклад, надійність, вартість, є обмеженими і постійними.

Одночасно з цим, кожна процедура АІБ ОБІ повинна враховувати його специфіку. Враховуємо ці індивідуальні критерії (метрики ІБ) в окремій множині. Індивідуальні критерії важливі виключно для конкретного ОБІ. Якщо хоча б один критеріїв не виконано, то стан захисту ОБІ не задовольняє необхідний рівень ІБ.

По-друге, у процесі модифікації БАІ зроблено таке припущення: порівняльна оцінка важливості загальних критеріїв може бути виконана за допомогою класичного експертного оцінювання. У цій ситуації немає необхідності вдаватися до задіяння парних порівнянь БАІ. Це стає можливим у силу тієї обставини, що чисельність загальних критеріїв щодо забезпечення ІБ ОБІ порівняно невелика. Як показала практика, для більшості практик забезпечення ІБ, вирішальними стають відібрані чотири – п'ять критеріїв (метрик ІБ).

По-третє, внесемо корективи в алгоритм обчислення синаптичних ваг входів нейронів. Значення синаптичних ваг входів нейронів, які відповідають кожному з порівнювальних об'єктів, розраховуємо, використовуючи систему нечітких правил типу IF-THEN. Правила побудовані на основі застосування методу Такагі-Сугено. Як вихідні дані подібної системи використовуємо критерії ІБ ОБІ, які відповідають цьому нейрону. Крім того, беремо до уваги індивідуальні критерії ІБ ОБІ.

Прийнято такі вихідні дані для модифікованого БАІ, який можна використовувати в процедурах аудиту ІБ ОБІ:

1) множина $\{Y_i\}, i \in [1,n]$, яка містить експертні оцінки важливості кожної з метрик ІБ, n – кількість критеріїв (метрик ІБ);

2) множина $\{Z_j\}$, $j \in [1,m]$, яка містить індивідуальні критерії (метрики ІБ) ОБІ, m – кількість індивідуальних критеріїв.

Виконання порівняльної оцінки важливості загальних критеріїв передбачає наступні етапи:

Етап 1. Керуючись необхідним рівнем ІБ ОБІ, експерт представляє важливість усіх загальних критеріїв ІБ у вигляді множини $\{Y_i\}, i \in [1,n]$, наприклад, для $Y \in [1,0]$, тут «0» відповідає ситуації, коли відсутні вимоги до ІБ об'єкта аудиту, а «10» – максимальна важливість критерію (за аналогією з МАІ Т. Сааті).

Етап 2. Перетворюємо множину $\{Y_i\}$ у множину $\{u_i\}$. Перетворення реалізуємо за рахунок нормалізації елементів $\{Y_i\}$ на інтервал $[0,1]$:

$$u_i = \frac{Y_i}{\sum_{j=1}^{n} Y_j}. \qquad (3)$$

Отримуємо множину $\{u_i\}$, яка буде містити порівняльні показники важливості загальних критеріїв ІБ, які аналізуються під час проведення АІБ ОБІ.

Нейронна мережа (НМ), яка використовується у ході обчислення рангів об'єктів аудиту, буде містити кількість нейронів h, що дорівнює числу об'єктів l, потенційно прийнятних у контурах захисту інформації та кібербезпеки ОБІ. Кожен із нейронів володіє кількістю входів, що дорівнює кількості загальних вимог n. На виході нейронів буде формуватися значення, яке і визначить ранг відповідного йому об'єкта аудиту.

База нечітких правил (БНП) відбору індивідуальних метрик аудиту ІБ, що дозволяє розрахувати синаптичні ваги входів кожного з нейронів, буде включати правила у вигляді:

$$\left\{R^k\right\}: IF\ (x_k\ this\ A_k)\ THEN\ w_k = c_k, \tag{4}$$

$$w_i = \frac{\sum_{k=1}^{K} \mu_{A_k} \cdot (x_k) \cdot w_k}{\sum_{k=1}^{K} \mu_{A_k} \cdot (x_k)} \cdot \prod_{j=1}^{m} \mu_{z_j} \cdot (z_j), \tag{5}$$

де $\{R^k\},\ k \in [1, K]$ – БНП, яка містить нечітких правил;

$c_k,\ k \in [1, K]$ – константа, яка залежить від конкретного правила $c_k \in (0,10]$;

$A_k = \{x_k, \mu_{Ak}(x_k)\},\ k \in [1, K]$ – нечіткі множини, які задані функціями належності $\mu_{Ak}(x_k)$ на безлічі можливих значень характеристик об'єкта аудиту ІБ, і відповідають загальним метрикам ІБ;

$x_k,\ k \in [1, K]$ – значення змінних, які характеризують властивості об'єкта аудиту ІБ, і відповідають реалізації загальних критеріїв по ІБ ОБІ;

$z = \{z_j, \mu_{zj}(z_j)\},\ j \in [1, m]$ – класична множина, що задається функціями належності $\mu_{Zj}(z_j)$, рівними 0 або 1. Ця множина описує значення властивостей об'єкта аудиту ІБ, які відповідають за реалізацію індивідуальних критеріїв (метрик ІБ);

$z_j,\ j \in [1, m]$ – змінні, які характеризують властивості об'єкта аудиту ІБ, відповідно до індивідуальних критеріїв;

$i,\ i \in [1, n]$ – номер входу відповідного нейрона.

Функції, розташовані в частині з оператором правил $THEN$, визначаємо як константи. Тоді, ці функції будуть приймати максимальні значення у випадках, якщо властивості об'єктів аудиту ІБ відповідають нечітким множинам. До таких нечітких множин можна віднести, наприклад, такі: інформація про результативність «миттєвих аудитів» ІБ; інформація про результативність аудитів усіх типів; інформація про інциденти ІБ; інформація про нові уподобання в політиці ІБ особи, яка приймає рішення і т. ін. У процесі досліджень було встановлено, що задіяння для лінгвістичної оцінки властивостей об'єкта аудиту ІБ лише п'яти, шести термів дозволить оцінювати об'єкт з досить великим ступенем. При цьому ми зберігаємо простоту й наочність моделі, досконалості класичний БАІ.

Множину індивідуальних критеріїв АІБ Z задаємо на множині групових та індивідуальних властивостей всіх об'єктів, які входять в контури ІБ ОБІ. Функція належності $\mu_{zj}(z_j)$ множини Z буде дорівнює одиниці для тих властивостей об'єктів АІБ, які забезпечують реалізацію індивідуальних критеріїв. Відповідно, нульове значення буде в разі всіх інших властивостей.

Множини Z індивідуальних критеріїв, які ставляться у відповідність окремим об'єктам АІБ, являють собою підмножини множини Z. У множину, яка відповідає конкретному об'єкту аудиту ІБ, входять лише ті індивідуальні критерії АІБ, які можуть бути пред'явлені до даного об'єкта контурів ІБ ОБІ.

У підсумку, модифікований БАІ можна концептуально реалізувати у вигляді такої нейро-нечіткої системи (рис. 2). Така схема має на увазі об’єднання нейронної мережі, у якій здійснюються порівняння об’єктів контурів ІБ, а також і нечіткої системи, яка заснована на застосуванні бази нечітких правил, описаних вище.

Нечітка система відповідно до розробленої схеми, буде здійснювати, обчислення синаптичних ваг w_i входів нейронів. При цьому враховуються і індивідуальні критерії (табл. 1), які відібрані для процедур аудиту ІБ конкретного ОБІ. На вхід нейро-нечіткої системи будуть подаватися в експертні оцінки важливості критеріїв для конкретного ОБІ, а на виході зчитуються ранги $p_1, \ldots, p_n$ об'єктів контурів ІБ.

Таблиця 1

Приклад формування загальних і індивідуальних метрик при проведенні аудиту ІБ

Загальні метрики ІБ	
1	Метрики, що характеризують хости і їх зв'язність
2	Відсоток критичних додатків
3	Середній час на усунення вразливості
…	….
N	Загальний виграш і Очікувані річні втрати
Індивідуальні метрики ІБ (відібрані для аудиту ІБ для конкретного ОБІ)	
1	Ймовірна міра вразливості, що показує наскільки ймовірне виникнення уразливості нульового дня за певний період часу
2	Забезпечення максимальної повноти переліку інформаційних активів, в аспекті додаткової інформації про загрози ІБ
3	Визначення ступеня реалізації заходів (засобів) забезпечення ІБ
…	….
M	Встановлений бізнес ризик

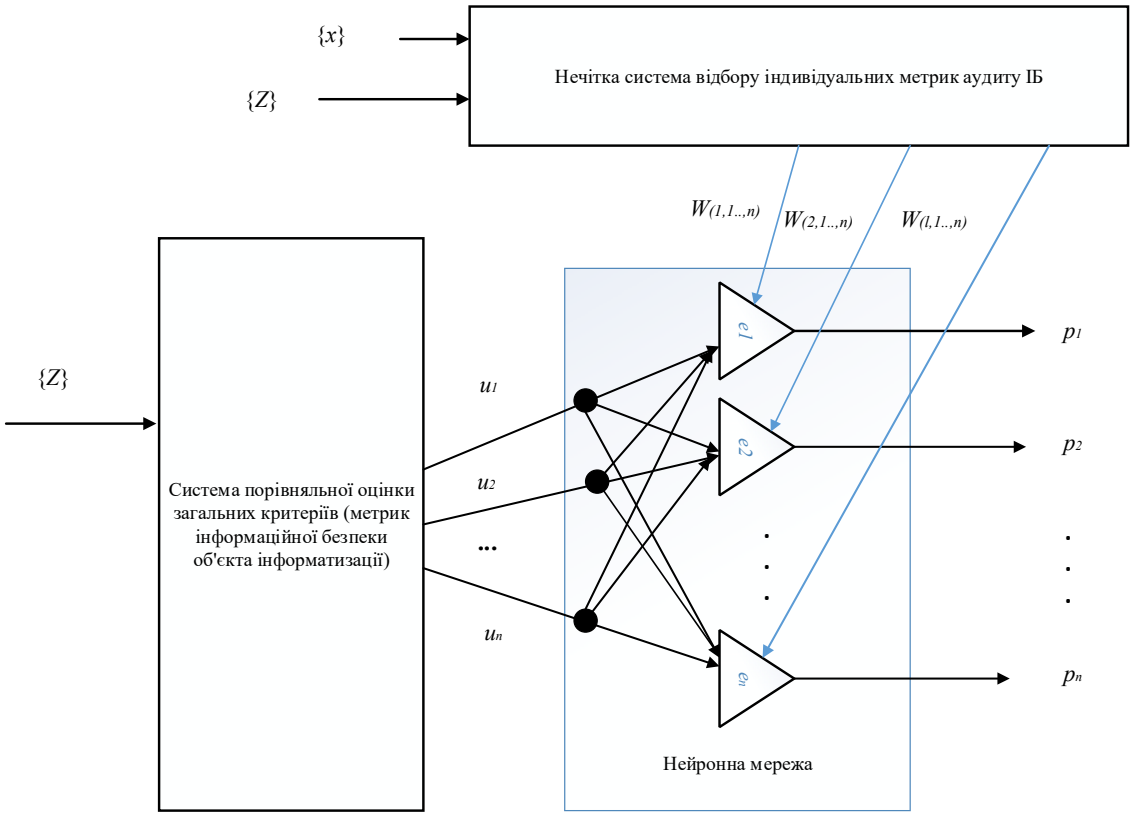


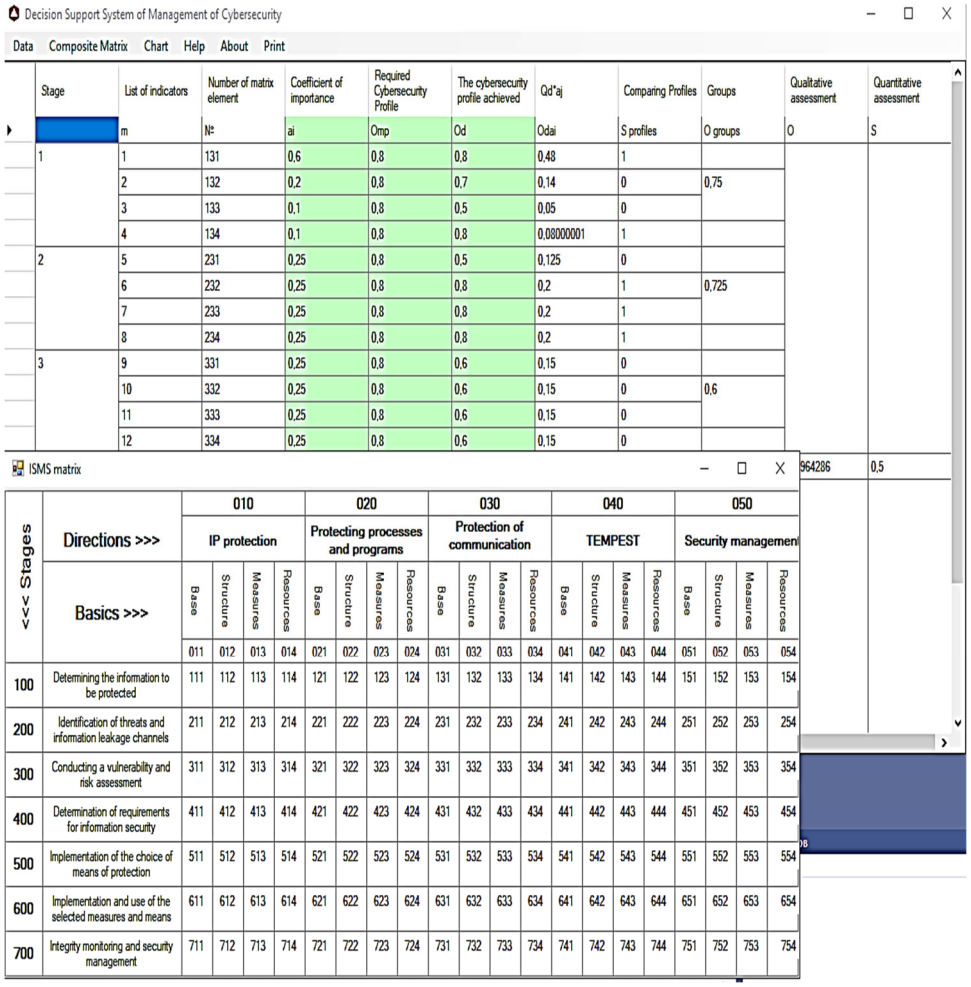
Рис. 2. Концептуальна структура нейро-нечіткої системи для модифікованого методу аналізу ієрархій

Програмна реалізація інтелектуальної СППР для аудиту інформаційної безпеки на основі застосування нейро-нечіткої системи

Описаний модифікований БАІ реалізований в системі Visual Studio 2019 (мова програмування С #) у вигляді інтелектуальної СППР для підвищення ефективності процедур аудиту ІБ (Рис. 3). Інтелектуальна СППР забезпечує введення індивідуальних критеріїв і експертних оцінок важливості загальних критеріїв, які перевіряються в ході аудиту ІБ ОБІ. Результати порівняння об'єктів представляються у вигляді графіка (рис. 4).

В основу досліджень, виконаних у межах цієї статті, були покладені ідеї, що дозволили гармонійно об'єднати теорію нейронних мереж і нечітких множин, методи прийняття рішень і метод аналізу ієрархій для проведення і вдосконалення процедур аудиту інформаційної безпеки різних об'єктів інформатизації.

Як видно на представленому графіку (рис. 4), застосування модифікованого БАІ дозволило отримати графік поточного стану ІБ обстеженого об'єкта інформатизації (лінія блакитного кольору). Причому відібрані критерії ІБ приблизно на 25-30 % нижче від еталонних значень. Хоча при застосуванні класичного БАІ не дало таких розбіжностей. Метод апробований в ході виконання аудитів ІБ ряду підприємств України і Казахстану.



Stage	List of indicators	Number of matrix element	Coefficient of importance	Required Cybersecurity Profile	The cybersecurity profile achieved	Qd*aj	Comparing Profiles	Groups	Qualitative assessment	Quantitative assessment
	m	№	ai	Omp	Od	Odai	S profiles	O groups	O	S
1	1	131	0,6	0,8	0,8	0,48	1			
	2	132	0,2	0,8	0,7	0,14	0	0,75		
	3	133	0,1	0,8	0,5	0,05	0			
	4	134	0,1	0,8	0,8	0,08000001	1			
2	5	231	0,25	0,8	0,5	0,125	0			
	6	232	0,25	0,8	0,8	0,2	1	0,725		
	7	233	0,25	0,8	0,8	0,2	1			
	8	234	0,25	0,8	0,8	0,2	1			
3	9	331	0,25	0,8	0,6	0,15	0			
	10	332	0,25	0,8	0,6	0,15	0	0,6		
	11	333	0,25	0,8	0,6	0,15	0			
	12	334	0,25	0,8	0,6	0,15	0		964286	0,5

<<< Stages	Directions >>>	010				020				030				040				050			
		IP protection				Protecting processes and programs				Protection of communication				TEMPEST				Security management			
	Basics >>>	Base	Structure	Measures	Resources	Base	Structure	Measures	Resources	Base	Structure	Measures	Resources	Base	Structure	Measures	Resources	Base	Structure	Measures	Resources
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Determining the information to be protected	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Identification of threats and information leakage channels	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Conducting a vulnerability and risk assessment	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Determination of requirements for information security	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Implementation of the choice of means of protection	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Implementation and use of the selected measures and means	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Integrity monitoring and security management	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Рис. 3. Загальний вигляд інтелектуальної СППР для аудиту інформаційної безпеки на основі застосування нейро-нечіткої системи

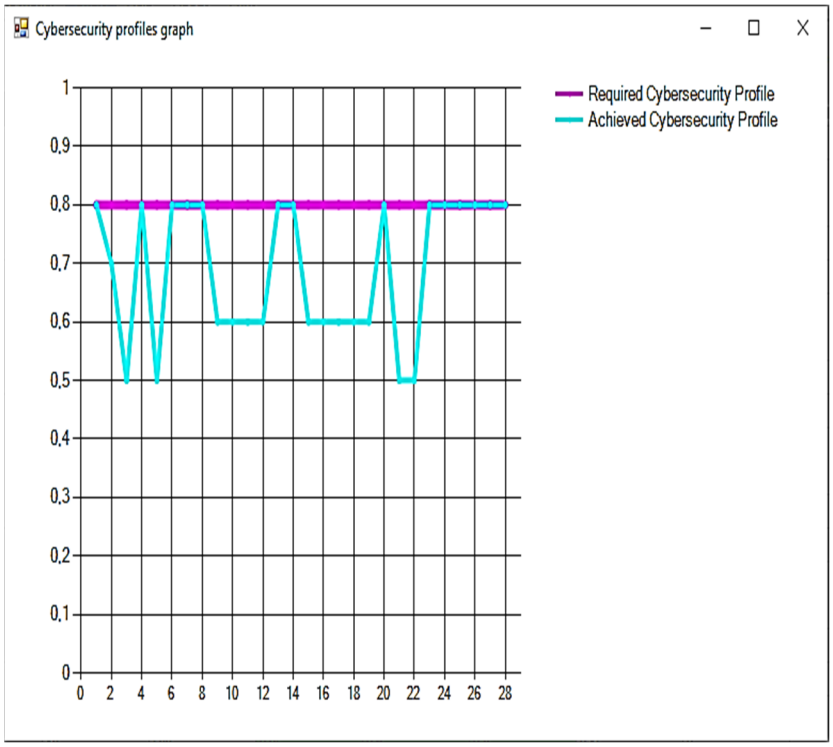


Рис. 4. Результати проведення аудиту ІБ ОБІ і зіставлення еталонних вимог до метрик ІБ і досягнутого рівня

Висновки. Проведені дослідження дозволяють зробити такі висновки:

1. Показано, що оцінку рівня ступеня інформаційної безпеки (ІБ) для об'єктів інформатизації (ОБІ) доцільно проводити на основі оцінювання результативності безлічі критеріїв методу аналізу ієрархій (МАІ). При цьому така оцінка ступеня ІБ і всі пов'язані з нею процедури аудиту ІБ (АІБ), найбільш ефективні для багатостороннього оцінювання ІБ ОБІ. Як метрики оцінювання можна використовувати як стандартні чисельні метрики ІБ, так і метрики, запропоновані експертами з ІБ і узгоджені з менеджментом ОБІ.

2. Запропоновано модифікований метод аналізу ієрархій, на основі застосування апарату теорії нечітких множин і нейронних мереж. Цей метод дає можливість менеджменту приймати обґрунтовані управлінські рішення у сфері ІБ ОБІ. Отримані рішення спрямовані на підвищення не тільки власне ІБ ОБІ, але й у кінцевому підсумку оптимізують систему управління ОБІ, скорочують витрати і підвищують ефективність бізнес-процесів ОБІ загалом. Представлений приклад розрахунку показників рівня ІБ умовного об'єкта інформатизації. Цей приклад ілюструє адекватність модифікованого МАІ.

3. Показано, що застосування математичного апарату МАІ і відповідного програмного забезпечення, зокрема, розробленої інтелектуальної системи, дозволяє підвищити ступінь достовірності результатів проведення комплексного аудиту ІБ ОБІ. Причому це твердження справедливо як для процедур внутрішнього АІБ ОБІ, так і для зовнішнього АІБ.

Список використаних джерел

1. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic / H. S. Lallie, L. A. Shepherd, J. R. Nurse, A. Erola, G. Epiphaniou, C. Maple, X. Bellekens // Computers & Security. – 2021. – № 105. – Art. 102248.

2. Miao Y. Machine Learning Based Cyber Attacks Targeting on Controlled Information: A Survey [Electronic resource] / Miao Y., Chen C., Pan L., Han Q. L., Zhang J., Xiang, Y. – 2021. – Assed mode: arXiv preprint arXiv:2102.07969.

3. Weaponized AI for cyber attacks / M. M. Yamin, M. Ullah, H. Ullah, B. Katt // Journal of Information Security and Applications. – 2021. – Vol. 57. Art. 102722.

4. Golyash I. Improving the information security audit of enterprise using XML technologies / I. Golyash, S. Sachenko, S. Rippa // Proceedings of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems. – 2011. – Vol. 2. – Pp. 795-798.

5. The influence of a good relationship between the internal audit and information security functions on information security outcomes / P. J. Steinbart, R. L. Raschke, G. Gal, W. N. Dilla // Accounting, Organizations and Society. – 2018. – № 71. – Pp. 15-29.

6. Griffiths P. Where next for information audit? / P. Griffiths // Business Information Review. – 2010. – Vol. 27(4). – Pp. 216-224.

7. The relationship between internal audit and information security: An exploratory investigation / P. J. Steinbart, R. L. Raschke, G. Gal, W. N. Dilla // International Journal of Accounting Information Systems. – 2012. – Vol. 13(3). – Pp. 228-243.

8. Kaur R. A survey on zero-day polymorphic worm detection techniques / R. Kaur, M. Singh // IEEE Communications Surveys & Tutorials. – 2014. – Vol. 16(3). – Pp. 1520-1549.

9. Steinbart P. J. Information security professionals' perceptions about the relationship between the information security and internal audit functions / P. J. Steinbart, R. L. Raschke, G. Gal, W. N. Dilla // Journal of Information Systems. – 2013. – Vol. 27(2). – Pp. 65-86.

10. Kayworth T. Effective information security requires a balance of social and technology factors / T. Kayworth, D. Whitten // MIS Quarterly executive. – 2010. – Vol. 9(3). – Pp. 2012-52.

11. Jarison, J., Morris, L., & Wilkinson, C. (2018). The future of cyber security in internal audit. Disponibil online la www. crowe. com/-/media/Crowe/LLP/foliopdf/The-Future-of-Cybersecurity-in-IA-Risk-18000-002A-update.ashx.

12. Suduc A. M. Audit for information systems security / A. M. Suduc, M. Bîzoi, F. G. Filip // Informatica Economica. – 2010. – Vol. 14(1). – P. 43.

13. Herath H. S. IT security auditing: A performance evaluation decision model / H. S. Herath, T. C. Herath // Decision Support Systems. – 2014. – Vol. 57. – Pp. 54-63.

14. Methodology and ontology of expert system for information security audit / L. B. Atymtayeva, G. K. Bortsova, A. Inoue, K. T. Kozhakhmet // the 6th International Conference on Soft Computing and Intelligent Systems, and The 13th International Symposium on Advanced Intelligence Systems. – IEEE, 2012, November. – Pp. 238-243.

15. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements, International Organization for Standardization, 2013.

16. ISO/IEC 27000:2014. Information technology. Security techniques. Information security management systems. Overview and vocabulary, International Organization for Standardization, 2014.

17. ISO/IEC 27004:2009. Information technology. Security techniques. Information security management systems. Measurement, International Organization for Standardization, 2009.

18. ISO/IEC 27005-2011 Information technology. Security techniques. Information security management systems. International Organization for Standardization, 2011.

19. ISO 19011:2011. Guidelines for auditing management systems. International Organization for Standardization, 2011.

20. Воеводин В. А. Эталонная модель объекта аудита информационной безопасности / В. А. Воеводин // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки. – 2019. – № 09. – С. 56-61.

21. Voevodin V. A. Method of The Study of Privacy Protection in Information / V. A. Voevodin // American Scientific Journal. – 2019. – Vol. 2, no. 32. – Pp. 47-51.

22. Voevodin V. A. Conceptual Model of Information Security Auditobject / V. A. Voevodin // Computational nanotechnology. – 2019. – No. 3. – Pp. 92-95.

23. Aguarón J. Consistency stability intervals for a judgement in AHP decision support systems / J. Aguarón, M.T. Escobar, J.M. Moreno-Jiménez // European Journal of Operational Research. – 2003. – Vol. 145, no. 2. – Pp. 382–393.

24. De Wilde P. Neural network models: theory and projects / P. De Wilde. – Springer Science & Business Media, 2013.

References

1. Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security, 105*, 102248.

2. Miao, Y., Chen, C., Pan, L., Han, Q. L., Zhang, J., & Xiang, Y. (2021). Machine Learning Based Cyber Attacks Targeting on Controlled Information: A Survey. arXiv preprint arXiv:2102.07969.

3. Yamin, M. M., Ullah, M., Ullah, H., & Katt, B. (2021). Weaponized AI for cyber attacks. *Journal of Information Security and Applications, 57*, 102722.

4. Golyash, I., Sachenko, S., & Rippa, S. (2011, September). Improving the information security audit of enterprise using XML technologies. In *Proceedings of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems* (Vol. 2, pp. 795-798). IEEE.

5. Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, *71*, 15-29.

6. Griffiths, P. (2010). Where next for information audit? *Business Information Review, 27*(4), 216-224.

7. Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012). The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems, 13*(3), 228-243.

8. Kaur, R., & Singh, M. (2014). A survey on zero-day polymorphic worm detection techniques. *IEEE Communications Surveys & Tutorials, 16*(3), 1520-1549.

9. Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2013). Information security professionals' perceptions about the relationship between the information security and internal audit functions. *Journal of Information Systems, 27*(2), 65-86.

10. Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly executive, 9*(3), 2012-52.

11. Jarison, J., Morris, L., & Wilkinson, C. (2018). *The future of cyber security in internal audit*. Disponibil online la www. crowe. com/-/media/Crowe/LLP/foliopdf/The-Future-of-Cybersecurity-in-IA-Risk-18000-002A-update.ashx.

12. Suduc, A. M., Bîzoi, M., & Filip, F. G. (2010). Audit for information systems security. *Informatica Economica, 14*(1), 43.

13. Herath, H. S., & Herath, T. C. (2014). IT security auditing: A performance evaluation decision model. *Decision Support Systems, 57*, 54-63.

14. Atymtayeva, L. B., Bortsova, G. K., Inoue, A., & Kozhakhmet, K. T. (2012, November). Methodology and ontology of expert system for information security audit. In *The 6th International Conference on Soft Computing and Intelligent Systems, and The 13th International Symposium on Advanced Intelligence Systems* (pp. 238-243). IEEE.

15. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements, International Organization for Standardization. (2013).

16. ISO/IEC 27000:2014. Information technology. Security techniques. Information security management systems. Overview and vocabulary, International Organization for Standardization. (2014).

17. ISO/IEC 27004:2009. Information technology. Security techniques. Information security management systems. Measurement, International Organization for Standardization. (2009).

18. ISO/IEC 27005-2011 Information technology. Security techniques. Information security management systems. International Organization for Standardization. (2011).

19. ISO 19011:2011. Guidelines for auditing management systems. International Organization for Standardization. (2011).

20. Voevodin, V. A. (2019). Etalonnaia model obekta audita informatsionnos bezopasnosti [Reference Model of an Information Security Audit Object]. *Modern Science: actual problems of theory and practice. Series of "Natural and Technical Sciences",* (9), 56-60.

21. Voevodin, V. A. (2019). Method of The Study of Privacy Protection in Information. *American Scientific Journal*, *2*(32), 47-51.

22. Voevodin, V. A. (2019). Conceptual Model of Information Security Auditobject. *Computational nanotechnology*, (3), 92-95.

23. Aguarón, J., Escobar, M.T., Moreno-Jiménez, J.M. (2003). Consistency stability intervals for a judgement in AHP decision support systems. *European Journal of Operational Research*, *145*(2), 382–393.

24. De Wilde, P. (2013). Neural network models: theory and projects. Springer Science & Business Media.

Отримано 18.07.2021

UDC 004.41.657

Valery Lakhno[1], Andriy Blozva[2], Yehor Chasnovskyi[3], Olena Kryvoruchko[4], Alona Desyatko[5]

[1]Doctor of Engineering, Professor, Head of Department of Computer Systems and Networks
National University of Life and Environmental Sciences of Ukraine (Kyiv, Ukraine)
E-mail: valss21@ukr.net. **ORCID:** http://orcid.org/0000-0001-9695-4543

[2]PhD of Pedagogical Sciences, Associate Professor, Associate Professor of the Department of Computer Systems and Networks
National University of Life and Environmental Sciences of Ukraine (Kyiv, Ukraine)
E-mail: andriy.blozva@nubip.edu.ua. **ORCID:** http://orcid.org/0000-0002-4377-0916

[3]PhD Student of the Department of Computer Systems and Networks
National University of Life and Environmental Sciences of Ukraine (Kyiv, Ukraine)
E-mail: egor.chasnovskii@gmail.com. **ORCID:** https://orcid.org/0000-0002-6360-4640

[4]Doctor of Engineering, Professor, Head of the Department of Software Engineering and Cyber Security
Kyiv National University of Trade and Economics (Kyiv, Ukraine)
E-mail: ev_kryvoruchko@ukr.net. **ORCID:** http://orcid.org//0000-0002-7661-9227

[5]PhD in Computer Sciences, Aassociate Professor of the Department of Software Engineering and Cyber Security
Kyiv National University of Trade and Economics (Kyiv, Ukraine)
E-mail: desyatko@knute.edu.ua. **ORCID:** https://orcid.org/0000-0002-2284-3218

INFORMATION SECURITY AUDIT BASED ON THE USE OF A NEURO-FUZZY SYSTEM

The article proposes measures to improve information security (IS) audit procedures (ISA) for various information objects (OBI). It is shown that the assessment of the IS for OBI level should be carried out based on assessing the effectiveness of many criteria of the method of analysis of hierarchies (MAH). At the same time, such an assessment of the degree of IS and all related AIB audit procedures are most effective for the multilateral assessment of IS OBI. Both standard numerical IS metrics and metrics proposed by IS experts and agreed with OBI management can be used as assessment metrics. A modified method of analysis of hierarchies is proposed, based on the application of the apparatus of fuzzy set theory and neural networks. This method allows management to make informed management decisions in the field of IS OBI. The obtained solutions are aimed not only at improving the OBI IB itself, but also, ultimately, optimizing the OBI management system, reducing costs, and increasing the efficiency of OBI business processes in general. It is shown that the use of the mathematical apparatus of MAH and the corresponding software, in particular, the developed intelligent system, allows increasing the degree of reliability of the results of a comprehensive audit of IB OBI. Moreover, this statement is valid for the procedures of the internal ISA OBI, as well as for the external ISA.

It is shown that it is expedient to assess the level of IS for OBI based on assessing the effectiveness of many criteria of the method of analysis of hierarchies. The algorithm of formalization of a typical problem of selection of ISA metrics is shown. The stages of building a hierarchy of IS metrics during the audit are identified. Given the specifics of the task of conducting an IS audit, changes are proposed to modify the MAH, which allows not only to take into account the specifics of the subject area of ISA OBI, but also further adaptation of the proposed changes for practical implementation.

Keywords: *information security audit; object of informatization; hierarchy analysis method; intelligent information system; neural networks; fuzzy logic.*

Fig.: 4. Table: 1. References: 24.

Лахно В., Блозва А., Часновський Є., Криворучко О., Десятко А. Аудит інформаційної безпеки на основі застосування нейро-нечіткої системи. *Технічні науки та технології.* 2021. № 3(25). С. 125-137.