DOI 10.20535/2411-1031.2025.13.1.328898
УДК 621.391:004.056.5

ВАДИМ АХРАМОВИЧ,
ВОЛОДИМИР АХРАМОВИЧ

МЕТОД РОЗРАХУНКУ ПОКАЗНИКА ЗАХИСТУ ІНФОРМАЦІЇ КОМ'ЮТЕРА В УМОВАХ НЕВИЗНАЧЕНОСТІ

Анотація. Найбільш вражаючою властивістю людського інтелекту є здатність приймати правильні рішення в умовах неповної і нечіткої інформації. Побудова моделей, які відтворюють мислення людини і використання їх у комп'ютерних системах на сьогодні є однією з найважливіших проблем науки.

Одним із ключових завдань аналізу та управління захистом інформації в сучасних комп'ютерах є обґрунтований вибір оптимального складу системних елементів, а також визначення їх параметрів таким чином, щоб забезпечити максимальну функціональну ефективність у складних умовах невизначеності. Це завдання набуває особливої актуальності у зв'язку зі зростанням складності комп'ютерів, а також через постійно змінювані умови функціонування та потенційні загрози безпеці. Правильний вибір елементів системи захисту інформації та їх параметрів дозволяє створити гнучку, адаптивну та надійну систему, яка здатна ефективно протидіяти ризикам навіть у випадках відсутності повної інформації про загрози. Таким чином, визначення складу елементів та їх параметрів є одним із базових етапів забезпечення інформаційної безпеки, який потребує застосування сучасних методів аналізу, моделювання та оцінювання

У цій статті проведено дослідження системи захищеності ком'ютера його складових в умовах невизначеності. Для цього складено: кортеж нечітких множин із складових ком'ютера; проведено його моделювання; розраховані рівні ризиків; рівні захищеності ком'ютера, агрегація результатів, функції належності. Для обрахунків параметрів, використані методи трапеції та трикутника. Розрахунки ілюстровані графічним матеріалом.

Підхід, реалізований у статті, дозволяє візуалізувати ступінь впевненості експерта в належності значень до обраного прийнятного показника захисту інформації в комп'ютері та відобразити цю впевненість за допомогою графіків і відповідних розрахунків. Запропонований метод розрахунку показника захисту включає процедури визначення цього показника з використанням трикутних і трапецієподібних показників, які відображають вплив складових комп'ютера.

Розроблений метод може бути ефективно використаний для вирішення завдань оцінювання показника захисту інформації комп'ютера, а також для подальшого вдосконалення методів аналізу інформаційної безпеки.

Ключові слова: показник захисту інформації, комп'ютер, нечіткі множини, кортеж, моделювання, ризики, агрегація, функція належності.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. У сучасному цифровому світі, де технологічний прогрес стрімко набирає обертів, забезпечення захисту інформації в комп'ютерах стає надзвичайно важливим завданням. Щодня зростає кількість кіберзагроз, які створюють ризики для окремих комп'ютерів, організаційних мереж, громадян і навіть національної безпеки. Особливої актуальності набувають задачі оцінювання кібербезпеки комп'ютера, ефективне вирішення яких залишається викликом для багатьох користувачів, адміністраторів мереж, керівників організацій і державних установ.

Зростаюча складність та варіативність кіберзагроз створюють суттєву невизначеність, що вимагає оцінки впливу складових комп'ютера на її загальну систему захисту. Це включає виявлення вразливостей, аналіз зовнішніх і внутрішніх ризиків, а також адаптацію заходів захисту до динамічно змінюваного ландшафту загроз.

Отже, розробка ефективних методів оцінювання та управління захистом інформації в комп'ютерах в умовах невизначеності є не лише технічною необхідністю, а й стратегічною потребою. Ці методи мають враховувати динамічну природу сучасних загроз, забезпечуючи стійкість систем і захист чутливої інформації в умовах все більш мінливого кіберпростору.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спирається автор, виділення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття.

Стаття [1] присв'ячена питанню кількісного визначення показника захищеності інформації на комп'ютері, в залежності від впливу на інформаційну структуру різних видів внутрішніх та зовнішніх загроз (відображає: ідентифікацію та автентифікацію користувачів, контроль цілісності та автентичності даних, резервне копіювання даних, розмежування доступу до інформації, роботу Firewall (пакетний фільтр), аудит, антивірусне забезпечення, збої та відмови компонент програмного та апаратного забезпечення, швидкості витоку інформації, вплив кількості інформації на їх витік, вплив загроз безпеки інформації від втрати довіри між користувачами, вплив розмірів системи комп'ютера на захищеність, вплив захищеності комп'ютера на витік інформації).Для вирішення вказаних завдань розроблена математична модель захисту інформації в ПК на основі системи диференціальних рівнянь та проведено моделювання рішень в системі MatLab. Розглянуті три варіанти вирішення рівняння близько стаціонарної стану системи (виконано більш наочний аналіз поведінки системи, з переходом від диференціальної форми рівнянь до дискретної і моделювання деякого інтервалу існування системи), зроблено висновок, що, виходячи з умов співвідношення дисипації і власної частоти коливань величини, загасання останньої до певного значення здійснюється періодично, з затухаючою амплітудою, або за експоненціально загасаючим законом.

Показано, що система захисту нелінійна, що потребує подальших досліджень.

В статті [1] показано, що система захисту ком'ютера є нелінійною, але вона не розглянута в нелінійній системі захисту, що являється недоліком, оскільки показник захисту не визначений достатньо точно..

В статті [2] відмічається, що один з актуальних напрямків, що розвиваються в області інформаційної безпеки, пов'язаний з використанням Honeypots (віртуальних приманок, онлайн-пасток), а вибір критеріїв для визначення найбільш ефективних Honeypot і їх подальшої класифікації є актуальним завданням. Представлені основні продукти, в яких реалізовані технології віртуальної приманки. Вони часто використовуються для вивчення поведінки, підходів і методів, які використовує стороння сторона для отримання несанкціонованого доступу до ресурсів інформаційної системи. Онлайн-хуки можуть імітувати будь-який ресурс, але частіше вони виглядають як справжні продакшн-сервери та робочі станції. Відомий ряд досить ефективних розробок, які використовуються для вирішення завдань виявлення атак на ресурси інформаційної системи, в основі яких лежить апарат нечітких множин. Вони показали ефективність відповідного математичного апарату, використання якого, наприклад, для формалізації підходу до формування набору еталонних значень, що дозволить поліпшити процес визначення найбільш ефективних Honeypots.

В статті [3] розглядається один із нових та перспективних підходів до вирішення проблеми оцінювання кібербезпеки на об'єктах критичної інфраструктури з використанням теорії нечітких множин, наприклад, для оцінки ризиків інформаційної безпеки. На практиці трапляються ситуації, коли на розрахунок кінцевих результатів істотно впливають невідповідності висновків або помилки експертів. Тому, щоб мінімізувати такі похибки, пропонується методи фазирування інтервалів шляхом перетворення їх у нечіткі числа.

В статті [4] для моделювання ризику інформаційної безпеки підприємства запропоновано нечіткі моделі надавати у вигляді нечітких мереж. Модель містить бази правил і дозволяє проводити лінгвістичний аналіз ризиків, які несуть потенційні загрози і збиток

організації. Використовуваний в методиці механізм отримання оцінок ризику на основі нечіткої логіки дозволяє отримати чисельне значення ризику, лінгвістичний опис ступеня ризику, а також рівень впевненості експерта у виникненні ризикової події.

Монографія [5] присвячена теоретико-методологічним і практичним аспектам розробки методів ідентифікації аномальних станів та методології побудови систем виявлення вторгнень. У роботі проведено аналіз засобів виявлення зловживань та аномалій. Значну увагу приділено формалізації процесу створення mi-вимірних параметричних, атакуючих, еталонних, поточних та детекційних середовищ. Це є підґрунтям для створення засобів, які дозволять автоматизувати процес детектування в слабоформалізованому нечітко визначеному середовищі аномальний стан, що породжується кібератаками, у заданий проміжок часу шляхом контролю поточного стану множини визначених параметрів. Такі засоби можуть використовуватися автономно або, як розширювач функціональних можливостей сучасних систем виявлення вторгнень.

В статті [6] відзначається, що одним з методів оцінки ризиків інформаційної безпеки є обґрунтований вибір і здійснення протидії загрозам. Ситуативна нечітка модель OWA багатокритеріальна. Вирішення проблеми вибору заходів протидії зниженню інформаційної безпеки пропонуються ризики. Запропонована модель дає можливість модифікувати пов'язані ваги критеріїв на основі інформаційної ентропії щодо ситуації агрегації. Перевагою модель полягає в постійному вдосконаленні вагових коефіцієнтів критеріїв і агрегації експертів. думки в залежності від параметра, що характеризує ситуацію агрегації.

В роботі [7] досліджується поєднання оцінку ризику (RA) і нечіткої логіки (FL), де: “Оцінка ризику – це загальний процес ідентифікації, аналізу та оцінки ризику. Ідентифікація ризику включає розуміння джерел ризику, сфер впливу, подій та їх причини та можливі наслідки. Мета полягає в тому, щоб створити вичерпний перелік ризиків, включаючи ризики, які можуть бути пов’язані з втраченими можливостями, і ризики, пов’язані з прямими контроль організації. Комплексний огляд дозволяє повністю розглянути потенціал вплив ризику на організацію”. “Нечітку логіку можна розглядати як спробу формалізації/механізації двох неабияких людських здібностей. По-перше, здатність розмовляти, міркувати та висловлюватися рішення в середовищі неточності, невизначеності, неповноти інформації, суперечлива інформація, частковість істини та частковість можливості – коротше кажучи, середовище недосконалої інформації. А по-друге, можливість виконувати різноманітні дії фізичних і розумових завдань без будь-яких вимірювань і будь-яких обчислень”. Мотивація для поєднання RA і FL виникає через те, що RA часто заважають дані обмеження та неоднозначності, такі як неповні або недостовірні дані та суб’єктивна інформація завдяки опорі на людей-експертів та їх передачу лінгвістичних змінних. Оскільки було показано, що моделі є ефективними інструментами за таких обставин, здається природним дослідити застосування RA FL. Зауважимо, що FL ідеально підходить для кількісної оцінки операційних і стратегічних ризиків.

У цій статті [8] розроблено підхід на основі аналізу оболонок даних (DEA) для вирішення MOSPP з нечіткими параметрами (FMOSPP) для врахування реальних ситуацій, коли вхідні–вихідні дані включають невизначеність трикутної форми членства. Цей підхід до встановлення зв'язку між MOSPP і DEA є більш гнучким для реального практичного застосування. У зв'язку з цим кожна дуга в FMOSPP розглядається як одиниця прийняття рішень з безліччю нечітких входів і виходів. Потім отримують дві нечіткі оцінки ефективності, що відповідають кожній дузі. Ці нечіткі оцінки ефективності об'єднані для визначення унікальної нечіткої відносної ефективності. Таким чином, FMOSPP перетворюється в одноцільову задачу нечіткого найкоротшого шляху (FSPP), яку можна вирішити за допомогою існуючих алгоритмів FSPP..

Стаття [9] відмічається, що багато реальних програм, що мають справу з вище зазначеними мережами, вимагають обчислення найкращих або найкоротших шляхів від одного вузла до іншого, що називається проблемою найкоротшого шляху (SPP). У цій роботі

запропоновано три нові алгоритми для задачі множинного об'єктивного найкоротшого шляху (MOSPP) та алгоритм виявлення негативного циклу в мережі. МОСПП у циклічній та ациклічній мережі, що має вагомості або позитивні, або негативні, або обидві можуть бути вирішені за допомогою запропонованих алгоритмів. Максимальне число оптимальних шляхів Парето MOSPP в мережі дуже корисно для знаходження максимального числа ітерацій і складності того чи іншого алгоритму. Використовується теорія нечітких множин

В статті [10] розглядаються різнітипи шкідливих атак, такі як електронні віруси, шкідливе програмне забезпечення, шкідливий код, та інші кіберзагрози, в першу чергу, які впливають на інформаційні системи. Системні адміністратори не знають типу та рівня атаки. Коли зловмисники зламують комп'ютерні системи, і вони не впевнені в діях, які необхідно вжити для захисту. Тому - наукові цілі визначити ці типи кібератак за допомогою теорії нечітких множині випустити попередження для адміністраторів, спонукаючи їх до вжиття необхідних дій.

В статті [11] описується кібербезпека промислової системи управління яка є дуже складна і складна тема дослідження, з огляду на інтеграцію цих систем у національні критичні інфраструктури. Системи управління зараз з'єднані між собою в промислові мережі і часто підключені до Інтернет. У цьому контексті вони стають мішенями різних кібератак зловмисників таких як хакери, промислові шпигуни тощо та розвідувальні служби. Автори пропонують спосіб моделювання профілів зловмисників і оцінки рівня успіху нападу, проведений у заданих умовах. Автори використовують нечіткий підхід для створення профілів зловмисників на основі атрибутів зловмисника, такі як знання, техресурсів і мотивації. Відсоток успішності атаки становить отримані за допомогою іншої системи нечіткого висновку, яка аналізує профіль зловмисника та внутрішні характеристики системи.

В роботі [12] наведено комплексний аналіз даних про вразливості критичної інфраструктури SCADA та використання алгоритмів нечіткого прийняття рішень. Ці алгоритми представлені в двох прикладах з описом можливих сценаріїв кібератаки на дві життєво важливі багатопараметричні системи дистанційного моніторингу. Головними об’єктами аналізу кібератак є дані, отримані з їх спільної системи SCADA. Результати нечіткого моделювання безпосередньо залежить від складного вибору правил якщо-то, на основі яких приймаються рішення. Крім того, дві системи нечіткої логіки (FLS-T1 і FLS-T2) використовуються для моделювання кількох сценаріїв кібератак.

В літературних джерелах [2]–[11] не розглядається розрахунок показника захищеності інформації ком’ютера, що являється недоліком.

Формулювання цілей статті.

Аналіз умов невизначеності в захисті інформації:

1. Провести дослідження природи невизначеності, яка виникає під час оцінювання захищеності інформації в комп’ютерах, зокрема через змінність та неповноту даних про загрози й уразливості.

2. Розробка методу оцінювання захищеності:

Запропонувати ефективний метод розрахунку показника захисту інформації в комп’ютері, який враховує вплив різних складових інформаційної системи та діє в умовах невизначеності.

3. Використання нечіткої логіки:

Застосувати інструменти нечіткої логіки для побудови моделей, які відображають взаємозв’язок між складовими комп’ютера та рівнем його захищеності.

4. Розробка процедур моделювання:

Розробити процедури моделювання ризиків, визначення рівня захищеності та агрегації результатів з використанням нечітких множин, функцій належності та методів трапеції й трикутника.

5. Ілюстрація практичного застосування:

Показати практичне застосування запропонованого методу через приклади графічних розрахунків, що демонструють ступінь впливу складових системи на загальний показник захищеності.

6. Сприяння розвитку кібербезпеки:

Забезпечити наукове підґрунтя для подальшого розвитку методів оцінювання кібербезпеки, що можуть бути використані для аналізу, прогнозування та покращення захисту інформації в комп'ютерах.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів.

Складання кортежа параметрів

Кортеж представлений як:

$$< I, Z, Z_p, C_v, C_k, C_{d1}, C_{d2}, Q, W, F, V, Z_{p1}, Z_k, I_d, A, R, A_d >, \quad (1)$$

де кожен елемент визначає специфічний аспект захисту інформації комп'ютера:

– I : *потік інформації* – визначає обсяг або частоту передачі інформації в системі (значення $0…1$);

– Z : *показник захищеності інформації* – відображає ефективність механізмів захисту (значення $0…1$);

– Z_p : *вплив заходів захисту* – визначає, наскільки заходи безпеки впливають на загальний рівень захисту (значення $0…1$);

– C_v : *вплив швидкості витоку даних* – чим більша швидкість витоку, тим більше загроза (значення $0…1$);

– C_k : *вплив обсягу даних на ризик витоку* – більший обсяг даних може призводити до підвищеного ризику (значення $0…1$);

– C_{d1} : *розміри системи* (значення $0…1$) – впливає на витік інформації;

– C_{d2} : *захищеність системи* (значення $0…1$) – впливає на захищеність системи;

– Q : *коефіцієнт, що відображає контроль цілісності та автентичності даних* (значення $0…1$);

– W : *коефіцієнт, що відображає розмежування доступу до інформації* (значення $0…1$);

– F : *коефіцієнт, що відображає роботу Firewall* (значення $0…1$);

– V : *коефіцієнт, що відображає антивірусне забезпечення* (значення $0…1$);

– Z_{p1} : *коефіцієнт, що відображає збої та відмови компонент програмного забезпечення* (значення 0 або1);

– Z_k : *коефіцієнт, що відображає збої та відмови компонент апаратного забезпечення* (значення 0 або1);

– I_d : *коефіцієнт, що відображає ідентифікацію користувачів* (значення 0 або 1);

– A : *коефіцієнт, що відображає автентифікацію користувачів* (значення 0 або 1);

– R : *коефіцієнт, що відображає резервне копіювання даних* (значення $0…1$);

– A_d : *коефіцієнт, що відображає аудит* – використовується для спостереження, протоколювання (значення $0…1$).

Щоб розв'язати задачу з нечіткими множинами та побудувати графіки для кожного аспекту на п'яти рівнях, розіб'ємо задачу на кілька кроків.

1. **Формалізація моделі нечітких множин**:

Для кожного параметра визначимо п’ятирівневу шкалу значень функції належності $\mu(x) \in \overline{0,1}$, наприклад:

- Дуже низький ($\mu(x) \in \overline{0,\ 0.2}$);
- Низький ($\mu(x) \in \overline{0.2,\ 0.4}$);
- Середній ($\mu(x) \in \overline{0.4,\ 0.6}$);
- Високий ($\mu(x) \in \overline{0.6,\ 0.8}$);
- Дуже високий ($\mu(x) \in \overline{0.8, 1.0}$).

2. **Вхідні дані**:

Розглянемо кортеж, що представляє показники захисту, як множину параметрів. Кожен параметр змінюється від 0 до 1 (або має фіксовані значення 0 або 1).

3. **Побудова графіків**:

Для кожного параметра створимо графіки функцій належності для п'яти рівнів.

4. **Презентація графіків**:

Побудуємо кожен графік у вигляді тріангульованих функцій належності, які ілюструють нечіткі рівні.

Приклад формули функцій належності нечіткої множини:

$$\mu(x) = \begin{cases} 0, & x < a \\ \dfrac{x-a}{b-a}, & a \le x \le b \\ 0, & x > c \end{cases},$$

де a, b, c – точки визначення тріангульованої функції для рівнів.

Нечітка множина “Середній рівень ризику”.

Параметри трикутника:

- $a = 0.25$: нижній поріг, де ризик починає зростати;
- $b = 0.5$: максимальне значення належності, тобто середній ризик;
- $c = 0.75$: верхній поріг, де середній ризик закінчується.

Тоді:

$$\mu_{\text{СР}}\ (x) = \begin{cases} 0, & x < 0.25 \text{ або } x > 0.75 \\ \dfrac{x-0.25}{0.5-0.25}, & 0.25 \le x < 0.5 \\ \dfrac{0.75-x}{0.75-0.5}, & 0.5 \le x < 0.75 \end{cases}.$$

Пояснення:

1) Якщо $x = 0.2$: $\mu(x) = 0$, оскільки $x < a$.

2) Якщо $x = 0.4$:

$$\mu(x) = \frac{x–0.25}{0.5–0.25} = \frac{0.4–0.25}{0.25} = 0.6$$

1) Якщо $x = 0.7$:

$$\mu(x) = \frac{0.75–x}{0.75–0.5} = \frac{0.75–0.7}{0.25} = 0.2$$

2) Якщо $x = 0.8$: $\mu(x) = 0$, оскільки $x > c$.

Ця формула дозволяє визначити ступінь належності значення x до рівня “Середній ризик”.

Отже, побудуємо функції належності для кожного параметра (рис. 1).

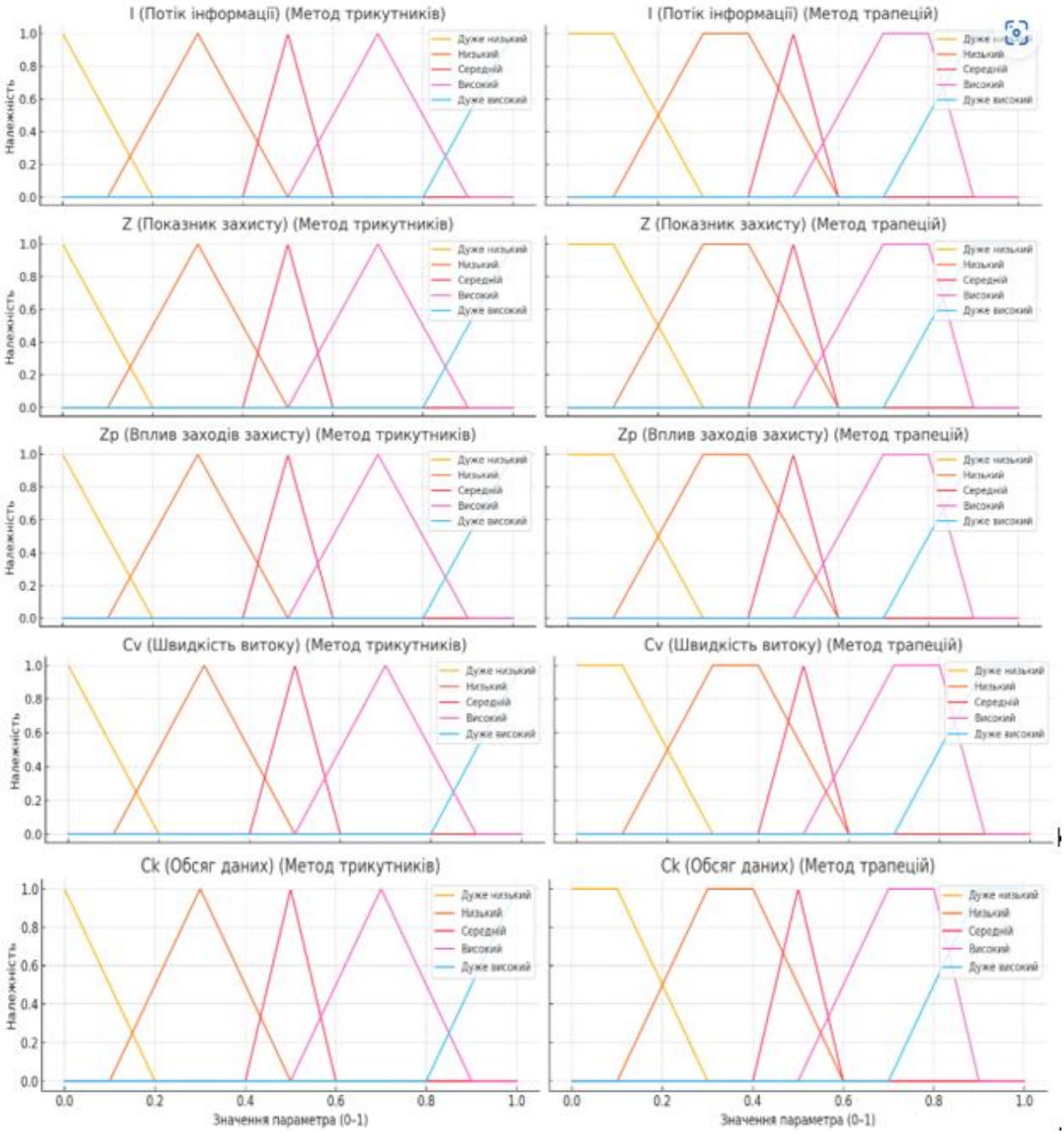

Рисунок 1 – Залежність складових кортежа від параметра *x*

Кожен графік демонструє функції належності для рівнів:

- Дуже низький;
- Низький;
- Середній;
- Високий;
- Дуже високийю

Ці рівні визначають нечіткі інтервали параметрів у діапазоні від 0 до 1. Можна використати ці графіки для аналізу показників захисту комп’ютера.

Методи трикутників і трапецій є популярними способами представлення нечітких множин. У методі *трикутників* використовуються тріангульовані функції належності для

опису поступового зростання і спаду належності в певному інтервалі. Метод *трапецій* дозволяє описувати нечіткі множини з більш широкими плато між двома рівнями.

При побудові графіків основними математичними залежностями наступні.

1. Функція належності для трикутної форми визначається наступною формулою:

$$\mu(x) = \begin{cases} 0, & x<a \text{ або } x>c \\ \frac{x-a}{c-b}, & a \le x \le b \\ \frac{c-x}{c-b}, & b \le x \le c \end{cases}, \quad (2)$$

де a – початок зростання належності (ліва межа);

b – вершина трикутника (максимальна належність, $\mu(x)=1$;

c – кінець зменшення належності (права межа).

2. Функція належності для трапецієподібної форми визначається таким чином:

$$\mu(x) = \begin{cases} 0, & x<a \text{ або } x>d \\ \frac{x-a}{b-a}, & a \le x \le b \\ 1, & b \le x \le c \\ \frac{d-x}{d-c}, & c \le x \le d \end{cases}, \quad (3)$$

де a – початок зростання належності (ліва межа);

b – початок плато (максимальна належність, $\mu(x)=1$;

c – кінець плато;

d – кінець зменшення належності (права межа).

Для кожного рівня нечіткої множини (“Дуже низький”, “Низький”, “Середній”, “Високий”, “Дуже високий”) визначено відповідні межі (a,b,c для трикутників та a,b,c,d для трапецій).

Інтерпретація графіків:

– вісь x: значення параметра (наприклад, захисту, витоку тощо), змінюється від 0 до 1;

– вісь у: ступінь належності $\mu(x)$ до певного рівня (наприклад, “Низький”);

– вершини та плато показують діапазони, де параметр найбільш відповідає певному рівню;

– метод *трикутників* (ліворуч): Показує поступове збільшення і зменшення належності в межах кожного рівня;

– метод *трапецій* (справа): Демонструє ширші плато для кожного рівня, що забезпечує стабільну належність у середніх діапазонах значень.

Розрахунок конкретних значень параметрів для кожного з аспектів захисту інформації комп'ютерної системи залежить від специфіки задачі. В основі лежать метрики, які можна отримати через моніторинг, аналіз або експертну оцінку. Наведемо математичні визначення параметрів кортежу (1).

Основні параметри:

– I : *потік інформації*– визначається як відношення реального обсягу переданих даних $I = \frac{V_{real}}{V_{\max}}$;

– Z : *показник захищеності інформації* (значення $0\ldots1$) – визначається як відношення кількості успішно захищених запитів *Rprotected* до загальної кількості запитів $Z = \frac{Rprotected}{Rtotal}$;

– Z_p: *вплив заходів захисту* (значення 0…1) – розраховується як ефективність використання реалізованих (*Eactual*) заходів безпеки до потенційно можливих (Epotential) $Z_p = \frac{Eactual}{Epotential}$.

Ризики та впливи:

– C_v: *вплив швидкості витоку даних* (значення 0…1) – Визначається як відношення швидкості витоку даних $V_{\max}$ – до максимально можливої $C_v = \frac{V_{lrak}}{V_{\max}}$;

– C_k: *вплив обсягу даних на ризик витоку* (значення 0…1) – відображає частку критичних даних серед загального обсягу $C_k = \frac{V_{critical}}{V_{total}}$.

Системні характеристики:

– C_{d1}: *розміри системи* (значення 0…1) – визначає залежність витоків від складності системи $C_{d1} = 1 - \frac{N_{leaks}}{N_{total}}$,

де N_{leaks} – кількість витоків, N_{total} – кількість елементів системи;

– C_{d2}: *захищеність системи* (значення 0…1) – визначає загальну захищеність системи $C_{d2} = \frac{N_{sekured}}{N_{total}}$.

Технологічні параметри:

– Q: *коефіцієнт, що відображає контроль цілісності та автентичності даних* (значення 0…1) – визначається як частка коректних даних серед усіх перевірених $Q = \frac{D_{valid}}{D_{total}}$;

– W: *коефіцієнт, що відображає розмежування доступу до інформації* (значення 0…1) $W = \frac{U_{correct}}{U_{total}}$,

де $U_{correct}$ – частка користувачів, що мають правильні доступи;

U_{total} – загальна кількість користувачів;

– F: *коефіцієнт, що відображає роботу Firewall* (значення 0…1) – відображає ефективність виявлення та блокування атак $F = \frac{A_{bloked}}{A_{total}}$;

– V: *коефіцієнт, що відображає антивірусне забезпечення* (значення 0…1) – частка успішно виявлених шкідливих програм $V = \frac{M_{detected}}{M_{total}}$.

Фіксовані параметри (0 або 1):

– Z_{p1}, Z_k, I_d, A: значення цих параметрів встановлюються на основі фактів (відмова компонента, ідентифікація/автентифікація користувача). Наприклад, $Z_{p1} = 1$ якщо програмне забезпечення працює без збоїв або $I_d = 1$ якщо користувача ідентифіковано;

– R: *коефіцієнт, що відображає резервне копіювання даних* (значення 0…1) – частка даних, які успішно резервовано $R = \frac{D_{backup}}{D_{total}}$;

– A_d: *коефіцієнт, що відображає аудит* – використовується для спостереження, протоколювання (значення 0…1).

Розрахунки базуються на фактичних даних або моделюванні процесів у системі.

Формалізація моделі захищенності інформації комп'ютера на основі нечітких множин.

Показник захищеності розраховується за формулою [1]:

$$Z = \frac{I_d A(R + A_d) - (C_v + C_k)}{(Z_p + Q + W + F + V + Z_{p1} + Z_k)(C_{d2} + C_{d1})}. \quad (4)$$

На рисунку 2 наведено графіки функцій належності показника Z з використанням методу трикутників (ліворуч) і методу трапецій (праворуч).

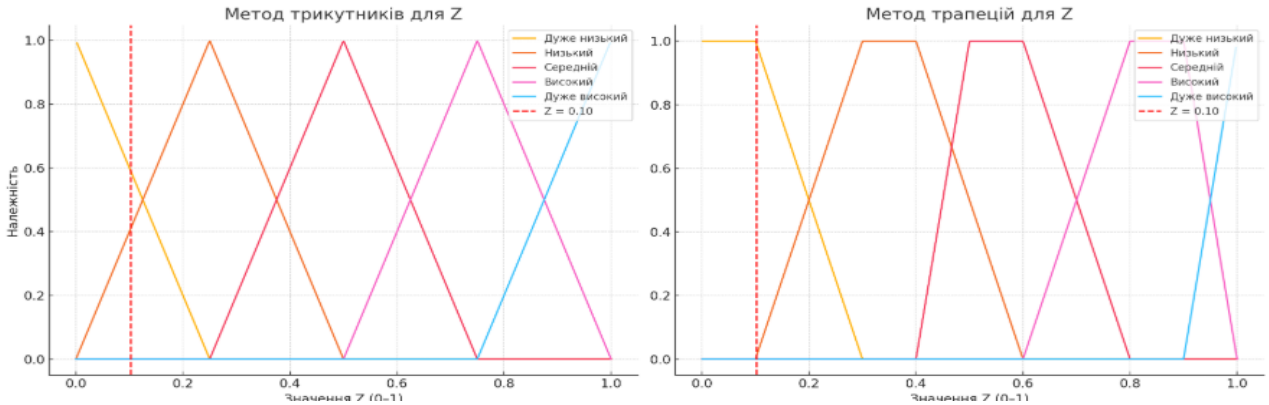

Рисунок 2 – Значення функції належності від параметра Z

Червона пунктирна лінія позначає значення Z, яке було обчислене за заданою формулою (4) та введеними параметрами.

Криві відповідають функціям належності для кожного рівня оцінки: "Дуже низький", "Низький", "Середній", "Високий", "Дуже високий".

Значення Z, обчислене за формулою, отримали 0.56. Це значення розташоване між рівнями "Середній" та "Високий", що видно на обох графіках.

Метод трикутників:

Крива належності "Середній" має максимальне значення на $Z \approx 0.5$, тому для $Z = 0.53$ рівень "Середній" ще є домінуючим, але вже з тенденцією до "Високий". Належність до "Середній" – приблизно 0.8, а до "Високий" – близько 0.2.

Метод трапецій:

Графік трапецій демонструє більш плавний перехід між рівнями. Значення $Z = 0.56$ перебуває у зоні перекриття рівнів "Середній" та "Високий". Належність до "Середній" більша (≈ 0.7), але "Високий" теж починає зростати (≈ 0.3).

Загальна інтерпретація:

1. Система знаходиться в **зоні середньої захищеності з тенденцією до високого рівня**.
2. Для покращення захисту варто підвищити значення таких параметрів, як:
   – Резервування (R): збільшити обсяги та якість резервного копіювання;
   – Аудит (A_d): посилити контроль і протоколювання дій;
   – Контроль доступу (W): зменшити ризики шляхом обмеження доступу.
3. Зменшення ризиків витоку даних (C_v, C_k) також допоможе підвищити загальний рівень захищеності.

Виконання пп.2, 3 допоможе значенню Z перемістити в зону "Високий".

Вихідні дані для розрахунку Z наведені у таблиці 1. **Результат**: $Z = \frac{0.9}{1.6} \approx 0.56$.

Таблиця 1 – Параметри для розрахунку показника захищеності інформації

Показник	Значення	Інтерпретація
I_d	1	Ідентифікація користувача активована
A	1	Автентифікація користувача активована
R	0.8	Резервне копіювання працює на високому рівні
A_d	0ю6	Аудит виконується на середньому рівні
C_v	0.3	Швидкість витоку даних помірна
C_k	0.2	Обсяг даних має невеликий вплив на ризики витоку
Z_p	0.7	Підвищення ефективності захисту
Q	0.8	Контроль цілісності даних працює на високому рівні
W	0.9	Доступ до інформації чітко розмежований
F	0.85	Firewall працює на високому рівні
V	0.75	Антивірусне забезпечення працює на високому рівні
Z_{p1}	1	Компоненти ПЗ не мають збоїв
Z_k	0	Збої апаратного забезпечення відсутні
C_{d1}	0.2	Розмір системи впливає на захищеність позитивно
C_{d2}	0.2	Розмір системи позитивно впливає на захищеність

Результати дефазифікації представлено на рис. 3.

Рисунок 3 – Дефазифікація показника впливу заходів захисту

Висновки і перспективи подальших досліджень. На рис. 2 представлено вплив значень Z на ступінь належності $\mu(x)$ до кожного рівня. Чим більше перекриття, тим більше сумарне значення початкових інтервалів, що відображаються у верхній основі трапеції для яких $\mu(x) = 1$. Цей підхід дозволяє візуалізувати ступінь впевненості експерта в належності значень до обраного прийнятного показника захищеності інформації в ком'ютерній системі та

відобразити цю впевненість на підставі графіків і відповідних розрахунків, що наведені в статті. Таким чином, запропонований метод розрахунку показника захищеності на основі трикутних та трапецієподібних функцій належності наочно представляє впливу окремих факторів на загальну захищеність комп'ютера.

Подальші дослідження будуть спрямовані на дослідження захищеності комп'ютерних мереж.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] В.М. Ахрамович, І.Г. Батрак, В.П. Коліда, та К.В. Шворак, "Показник захищеності інформації окремого комп'ютера", *Телекомунікаційні та інформаційні технології*, № 4 (73), с. 62-77, 2021, doi: https://doi.org/10.31673/2412-4338.2021.046277.

[2] A. Korchenko et al., "Development of a method for constructing linguistic standards for multi-criteria assessment of honeypot efficiency", *Eastern European Journal of Enterprise Technologies*, vol. 111, iss. 3 (9), pp. 63-83, 2021, doi: https://doi.org/10.15587/1729-4061.2021.225346.

[3] С.П. Євсеєв, О.В. Шматко, Н.В. Ромащенко, "Алгоритм оцінювання ступеня ризику інформаційної безпеки, що базується на нечіткомножинному підході", *Сучасні інформаційні системи*, т. 3, № 2, с. 73-79, 2019.

[4] О.В. Кочетков, Т.О. Гаур, та В.М. Машін, "Система оцінки ризиків інформаційної безпеки підприємства на основі нечіткої логіки", *Наукові праці ОНАЗ ім. О.С. Попова*, № 1, с. 97-104, 2019, doi: https://doi.org/10.33243/2518-7139-2019-1-1-97-104.

[5] А.О. Корченко, *Методи ідентифікації аномальних станів для систем виявлення вторгнень, Монографія*. Київ, Україна: ЦП "Компринт", 2019.

[6] Y.N. Imamverdiyev, and S.A. Derakshande, "Fuzzy Owa Model for Information Security Risk Management", *Automatic Control and Computer Sciences*, vol. 45, no. 1, pp. 20-28. 2021. [Online]. Available: https://www.researchgate.net/publication/265520240_Fuzzy_Owa_Model_for_Information_Security_Risk_Management_YN_Imamverdiyev_SA_Derakshande_Automatic_Control_and_Computer_Sciences_45_1_20-28. Accessed on: Jan. 04, 2025.

[7] M. Bagheri, A. Ebrahimnejad, S. Razavyan, F. Hosseinzadeh, and N. Malekmohammadi, "Solving fuzzy multi-objective shortest path problem based on data envelopment analysis approach", *Complex & Intelligent Systems*, vol. 7, pp. 725-740, 2021, doi: https://doi.org/10.1007/s40747-020-00234-4.

[8] V.N Sastry, T.N Janakiraman, and S.I. Mohideen, "New algorithms for multi objective shortest path problem", *Opsearch*, vol. 40 (4), pp. 278-298, 2003. [Online]. Available: https://link.springer.com/article/10.1007/bf03398701. Accessed on: Jan. 04, 2025.

[9] M. Mynuddin, M.I. Hossain, S.U. Khan, M.A. Islam, D.M.A. Ahad, and M.S. Tanvir, "Cyber Security System Using Fuzzy Logic", *Int. Conf. on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME 2023)*, Tenerife, Spain, 2023, pp. 1-6 doi: https://doi.org/10.1109/ICECCME57830.2023.10252778.

[10] E. Pricop, and S.F. Mihalache, "Fuzzy approach on modelling cyber attacks patterns on data transfer in industrial control systems", in *Proc. 7th Int. Conf. Elect., Comp. and AI (ECAI 2019)*, Bucharest, România, 2015, pp. 1-6. [Online]. Available: https://arxiv.org/pdf/1912.00234. Accessed on: Jan. 09, 2025.

[11] S.D. Milić, "Fuzzy-Decision Algorithms for Cyber Security Analysis of Advanced SCADA and Remote Monitoring Systems. Chapter 7" in *Cyber Security of Industrial Control Systems*

in the Future Internet Environment, M.D. Stojanović and S.V.Boštjančič Rakas, Eds. IGI Global Scientific Publishing Platform, doi: https://doi.org/10.4018/978-1-7998-2910-2.ch007.

Стаття надійшла до редакції 18.01.2025.

REFERENCES

[1] V.M. Akhramovych, I.H. Batrak, V.P. Kolida, and K.V. Shvorak, "Indicator of information security for an individual computer", *Telecommunications and Information Technologies*, no. 4 (73), pp. 62-77, 2021, doi: https://doi.org/10.31673/2412-4338.2021.046277.

[2] A. Korchenko et al., "Development of a method for constructing linguistic standards for multi-criteria assessment of honeypot efficiency", *Eastern European Journal of Enterprise Technologies*, vol. 111, iss. 3 (9), pp. 63-83, 2021, doi: https://doi.org/10.15587/1729-4061.2021.225346.

[3] S.P. Yevseiev, O.V. Shmatko, and N.V. Romashchenko, "Algorithm for assessing the degree of information security risk based on the fuzzy set approach", *Modern Information Systems*, vol. 3, no. 2, pp. 73-79, 2019.

[4] O.V. Kochetkov, T.O. Gaur, V.M. Mashin, "Enterprise information security risk assessment system based on fuzzy logic", *Proceedings of the O.S. Popov ONAT*, no. 1, pp. 97-104, 2019, doi: https://doi.org/10.33243/2518-7139-2019-1-1-97-104.

[5] A.O. Korchenko, *Methods for identifying anomalous states for intrusion detection systems, Monograph*. Kyiv, Ukraine: CP "Komprint", 2019.

[6] Y.N. Imamverdiyev, and S.A. Derakshande, "Fuzzy Owa Model for Information Security Risk Management", *Automatic Control and Computer Sciences*, vol. 45, no. 1, pp. 20-28. 2021. [Online]. Available: https://www.researchgate.net/publication/265520240_Fuzzy_Owa_Model_for_Information_Security_Risk_Management_YN_Imamverdiyev_SA_Derakshande_Automatic_Control_and_Computer_Sciences_45_1_20-28. Accessed on: Jan. 04, 2025.

[7] M. Bagheri, A. Ebrahimnejad, S. Razavyan, F. Hosseinzadeh, and N. Malekmohammadi, "Solving fuzzy multi-objective shortest path problem based on data envelopment analysis approach", *Complex & Intelligent Systems*, vol. 7, pp. 725-740, 2021, doi: https://doi.org/10.1007/s40747-020-00234-4.

[8] V.N Sastry, T.N Janakiraman, and S.I. Mohideen, "New algorithms for multi objective shortest path problem", *Opsearch*, vol. 40 (4), pp. 278-298, 2003. [Online]. Available: https://link.springer.com/article/10.1007/bf03398701. Accessed on: Jan. 04, 2025.

[9] M. Mynuddin, M.I. Hossain, S.U. Khan, M.A. Islam, D.M.A. Ahad, and M.S. Tanvir, "Cyber Security System Using Fuzzy Logic", *Int. Conf. on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME 2023)*, Tenerife, Spain, 2023, pp. 1-6 doi: https://doi.org/10.1109/ICECCME57830.2023.10252778.

[10] E. Pricop, and S.F. Mihalache, "Fuzzy approach on modelling cyber attacks patterns on data transfer in industrial control systems", in *Proc. 7th Int. Conf. Elect., Comp. and AI (ECAI 2019)*, Bucharest, România, 2015, pp. 1-6. [Online]. Available: https://arxiv.org/pdf/1912.00234. Accessed on: Jan. 09, 2025.

[11] S.D. Milić, "Fuzzy-Decision Algorithms for Cyber Security Analysis of Advanced SCADA and Remote Monitoring Systems. Chapter 7" in *Cyber Security of Industrial Control Systems in the Future Internet Environment*, M.D. Stojanović and S.V.Boštjančič Rakas, Eds. IGI Global Scientific Publishing Platform, doi: https://doi.org/10.4018/978-1-7998-2910-2.ch007.

VADYM AKHRAMOVYCH,
VOLODYMYR AKHRAMOVYCH

METHOD FOR CALCULATING THE COMPUTER INFORMATION PROTECTION INDEX UNDER CONDITIONS OF UNCERTAINTY

Abstract. The most striking property of human intelligence is the ability to make correct decisions under conditions of incomplete and uncertain information. Building models that replicate human thinking and applying them in computer systems is currently one of the most critical challenges in science.

One of the key tasks in analyzing and managing information security in modern computers is the justified selection of the optimal set of system elements and determining their parameters in such a way as to ensure maximum functional efficiency under complex conditions of uncertainty. This task becomes particularly relevant due to the increasing complexity of computers and constantly changing operating conditions and potential security threats. A proper choice of information security system elements and their parameters allows for creating a flexible, adaptive, and reliable system capable of effectively countering risks, even in cases where complete information about the threats is unavailable. Therefore, determining the composition of elements and their parameters is one of the fundamental stages of ensuring information security, requiring the application of modern methods of analysis, modeling, and evaluation.

This paper investigates the security system of a computer and its components under conditions of uncertainty. To achieve this, a tuple of fuzzy sets comprising computer components was constructed, modeled, and analyzed. Risk levels and computer security levels were calculated, along with the aggregation of results and membership functions. Trapezoidal and triangular methods were applied to calculate parameters. The calculations are illustrated with graphical material.

The approach implemented in this study enables the visualization of an expert's confidence in the membership of values to the selected acceptable indicator of computer information security and represents this confidence through graphs and corresponding calculations. The proposed method for calculating the security indicator includes procedures for determining this indicator using triangular and trapezoidal metrics, reflecting the impact of computer components.

The developed method can be effectively used for solving tasks related to assessing the information security indicator of a computer, as well as for further improving methods of information security analysis.

Keywords: information security indicator, computer, fuzzy sets, tuple, modeling, risks, aggregation, membership function.

Ахрамович Вадим Володимирович, завідувач комп’ютерним центром, Національна академія статистики, обліку та аудиту, Київ, Україна. ORCID 0009-0003-2787-8745, 12zstzi@gmail.com.

Ахрамович Володимир Миколайович, д.т.н., проф., професор кафедри Систем інформаційного та кібернетичного захисту, Державнийо університет інформаційно-комунікаційних технологій, Київ, Україна. ORCID 0000-0002-0086-9131, 12z@ukr.net.

Akhramovych Vadym, head of the computing center, National academy of statistics, accounting and auditing, Kyiv, Ukraine.

Akhramovych Volodymyr, doctor of technical sciences, professor, professor at the academic department of information and cyber defense systems, State university of telecommunications, Kyiv, Ukraine.