method. Essence of this method, his actuality, requirements to realization, opens up in this article. Authors offer developed by them as a programming code of protection of the personal data in the environment of MS SQL Server.
**Keywords:** data base, personal data, protection of the personal data, data masking, confidential data, information system.

**Коломыщев Михаил Владимирович,** кандидат технических наук, доцент, доцент кафедры информационной безопасности Национального технического университета Украины «Киевский политехнический институт».
E-mail: box144a@ukr.net
**Коломицев Михайло Володимирович,** кандидат технічних наук, доцент, доцент кафедри інформаційної безпеки Національного технічного університету України «Київський політехнічний інститут».
**Kolomytsev Mykhailo**, PhD, reader of Information Security Cathedra, National Technical University of Ukraine «Kiev Polytechnic Institute».

**Южаков Анатолий Михайлович,** техник отдела информатизации департамента перспективного развития Национального технического университета Украины «Киевский политехнический институт».
E-mail: conf@pti.kpi.ua
**Южаков Анатолій Михайлович,** технік відділу інформатизації департаменту перспективного розвитку Національного технічного університету України «Київський політехнічний інститут».
**Yuzhakov Anatoly**, technician of Informatization Department, National Technical University of Ukraine «Kiev Polytechnic Institute».

**УДК 004.056.53:004.492.3 (045)**

# МЕТОД ВИЯВЛЕННЯ ТА ІДЕНТИФІКАЦІЇ ПОРУШНИКА В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

***Анна Корченко, Світлана Казмірчук, Андрій Гізун, Владислава Волянська, Сергій Гнатюк***

*Забезпечення безпеки державних інформаційних ресурсів нерозривно пов'язане з виявленням діяльності порушника інформаційної безпеки (ІБ) в інформаційно-комунікаційних системах (ІКС), в яких циркулює інформація з обмеженим доступом. Недоліком сучасних систем виявлення порушника ІБ, побудованих на евристичних правилах (ЕП) в тому, що вони в основному орієнтовані на використання таких математичних моделей, які вимагають багато часу на підготовку статистичних даних. Математичні моделі, засновані на експертних підходах, у цьому відношенні є більш ефективними. Пропонується метод, що дозволяє на основі суджень експерта в нечітких умовах розв'язати задачу виявлення та ідентифікації порушника (ВІП) в ІКС. У методі використовуються елементи нечіткої логіки для попереднього прийняття рішення про порушення та ідентифікацію особи порушника, а також базис звичайної чіткої логіки, що забезпечує уточнюючу інформацію. Метод включає етапи: формування коефіцієнтів важливості, множин категорій порушника та параметрів, еталонів нечітких параметрів, множини ЕП, зв'язок категорії порушника з параметрами; формування та фазифікації параметрів, обробки і формування кортежів параметрів; формування результату. Робота методу організована у 3 фази: підготовча; робота з нечіткими параметрами; робота з чіткими параметрами. Засновуючись на цьому методі може бути синтезована система ВІП, що базується на ЕП і характеризується високою ефективністю роботи в умовах нечіткості.*
***Ключові слова**: системи виявлення порушника, порушник інформаційної безпеки, ідентифікація, виявлення аномалій в інформаційно-комунікаційних системах, метод, нечітка логіка, базова модель ідентифікації порушника, логіко-лінгвістична зв'язка, евристичні правила, експертна оцінка.*

Однією з головних складових національної безпеки держави є інформаційна безпека (ІБ), яка визначається сукупністю різноманітних характеристик та категорій у сфері захисту інформації. У цьому аспекті вагоме місце займає такий напрям як захист державних інформаційних ресурсів (ДІР). Враховуючи стрімкий розвиток інформаційних технологій, що впливає як на захисні механізми, так і на засоби проведення інформаційних атак, набір можливих дій порушника значно збільшується. Безперервно зростає кількість порушників (неавторизованих сторін – НАС), загроз ІБ, а також проводяться принципово нові кібератаки на інформаційні ресурси, що ускладнює реалізацію ефективного захисту. Досягнення максимального ефекту захищеності ДІР можливе за умови того, що потенційні порушники ІБ (ППБ) відомі і це створює передумови для підбору та застосування

найбільш адекватних заходів та засобів захисту. Дана задача ускладнюється тим, що атаки на ДІР здійснюються в умовах, що характеризуються великим показником нестабільності, випадковості та непередбачуваності і таким чином інформаційно-комунікаційні системи (ІКС), в яких циркулюють і атакуються ДІР, є нечітко визначеним слабоформалізованим середовищем (НВСС). На сьогодні для захисту ресурсів ІКС застосовуються системи виявлення вторгнень, а в аспекті виявлення факту порушення ІБ – системи виявлення порушника. Практично вони всі побудовані на сигнатурному принципі і є не ефективними в умовах нечіткості вхідних даних (ВхД) [1]. З огляду на це, доцільним є розробка систем, що працюють на основі евристичних правил (ЕП), які в свою чергу потребують великої вибірки статистичних даних, що значно збільшує вимоги до часових та обчислювальних ресурсів таких систем. Цю проблему може вирішити застосування методів нечіткої логіки (НЛ). Тому розробка методу виявлення та ідентифікації порушника (ВІП) в ІКС на основі методів та моделей нечітких множин, який дозволить підвищити ефективність функціонування відповідних засобів є актуальною задачею.

У роботах [2-4] показана ефективність застосування математичного апарату НЛ для розв'язання задач, пов'язаних з виявленням атак на інформаційні ресурси та ПІБ в НВСС. У роботі [5] були виділені основні категорії ПІБ та параметри для ВІП, а в [6] розроблена модель еталонів лінгвістичних змінних для параметрів нечіткого характеру, які за рахунок формування множин пар «порушник $\rightarrow$ параметр» і «порушник $\rightarrow$ набір логіко-лінгвістичних зв'язок» дозволяють формалізувати процеси виявлення НАС у НВСС. Також, у роботі [7] сформовані ЕП, які, за рахунок множини еталонних параметрів, дозволяють виявити ознаки діяльності порушника і визначити його тип з певним показником небезпеки, породженої можливою атакою. У зв'язку з цим, метою роботи є розробка методу ВІП ІБ в ІКС, на основі якого можна синтезувати систему виявлення НАС, що підвищить ефективність функціонування відповідних засобів НВСС.

Запропонований метод розв'язує задачу ВІП в ІКС, процеси в яких при впливі НАС за своєю суттю є слабоформалізованими та нечіткими. Для реалізації методу використовуються елементи НЛ (для попереднього прийняття рішення про порушення та для ідентифікації особи порушника) та базис звичайної чіткої логіки (для уточнюючої ідентифікації). Метод має 3 фази: 1) підготовча фаза; 2) фаза роботи з нечіткими параметрами (НП); 3) фаза роботи з чіткими параметрами, які в свою чергу, складаються з окремих етапів. Розглянемо метод більш детально (його схематичне зображення наведено на рис. 1).

Перша фаза призначена для організації роботи системи ВІП в ІКС, її налаштування та визначення ВхД. Обробка нечітких даних при розв'язанні поставленої задачі супроводжується необхідністю формування функції належності (ФН), для чого застосуємо метод лінгвістичних термів з використанням статистичних даних (МЛТС), для реалізації операцій нечіткої арифметики (НА) – метод лінійної апроксимації по локальним максимумам (ЛАЛМ), а порівняння ФН – метод $\alpha$-рівневої відстані (АРВ) [2]. У першій фазі реалізовані етапи 1-4.

**Етап 1 – вибір методу визначення коефіцієнтів важливості (МВКВ).** На цьому етапі проходить вибір МВКВ із заданої множини, що використовується у подальшому для формування ЕП. Так, у роботі [8] розглянуто 25 МВКВ ($МВКВ_1$, $МВКВ_2$, …, $МВКВ_{25}$, наприклад, метод середніх рангів (СР), мультиплікативна згортка Кіні (МЗК), метод випадкових векторів (ВПВ) тощо), серед яких вибирається робочий метод. На його вибір впливають такі критерії як форма представлення ВхД і вихідних даних (ВихД), трудомісткість та рекомендована шкала [8]. Якщо заданим критеріям відповідають декілька методів, то остаточний вибір здійснюється за рішенням експерта. Наприклад, відповідно до заданих критеріїв і пріоритетів з множини $МВКВ_i$ ($i = \overline{1,25}$) вибирається метод середніх рангів.

**Етап 2 – формування множин категорій порушника та параметрів.** Етап орієнтований на визначення множин категорій порушника та параметрів, які використовуються для виявлення НАС. На основі аналізу середовища ІКС формуються ідентифікатори порушника для $k$-ого вузла $I_i^k$ ($i = \overline{1,n}$, $k = \overline{1,l}$), а також множини контрольованих нечітких $P_i^k$ та чітких параметрів $SP_i^k$ ($i = \overline{1,m}$, $k = \overline{1,l}$) і з певною, заздалегідь встановленою, періодичністю їх поточні значення, що заносяться у регістри системи ВІП.

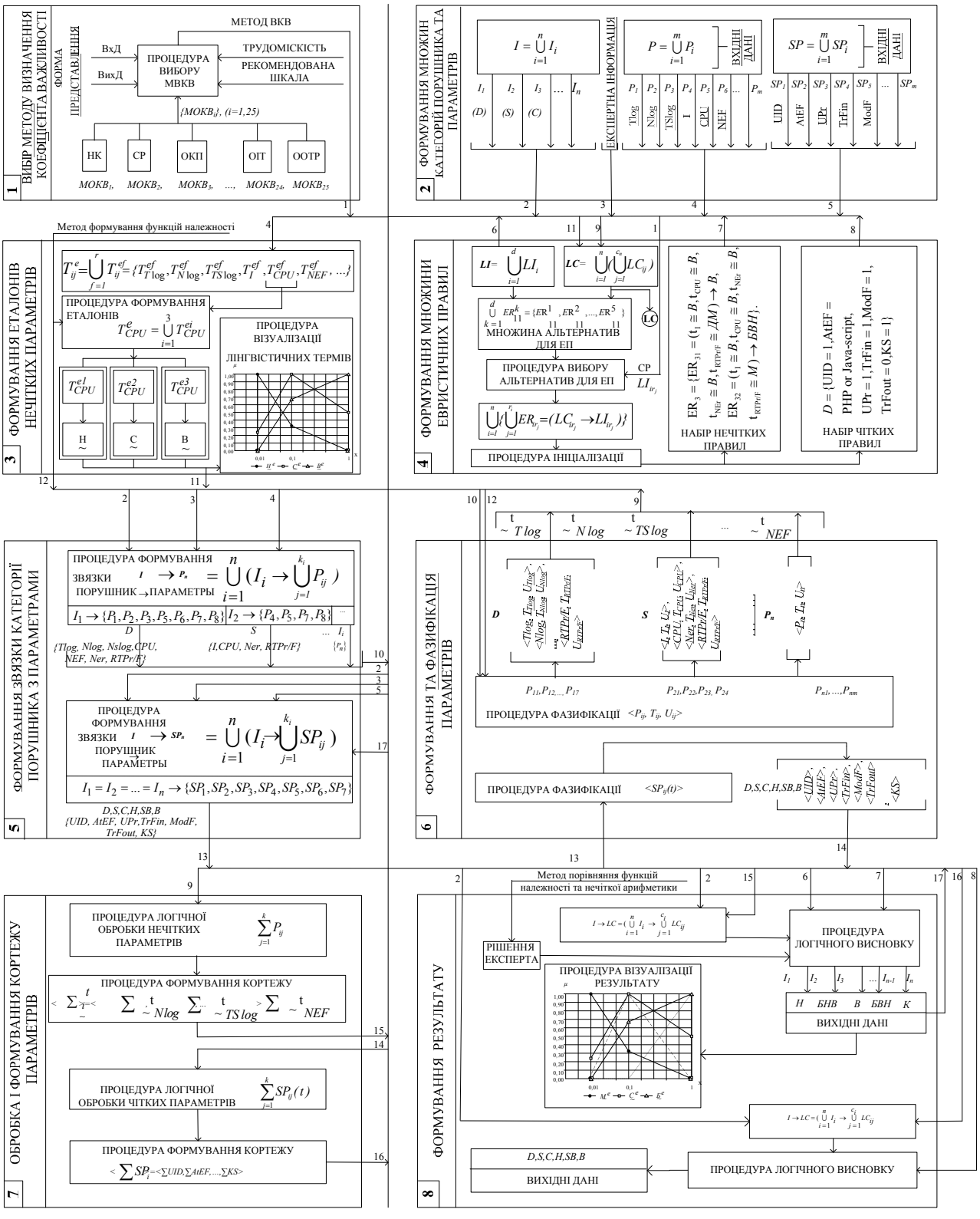


Рис.1. Метод ВІП в ІКС

Також, відповідно фіксуються параметри $I_i^k$, $P_i^k$ і $SP_i^k$, які дозволяють виявити ознаки діяльності шести видів НАС $I_1^k$, $I_2^k$, $I_3^k$, $I_4^k$, $I_5^k$ і $I_6^k$ ($D^k$, $S^k$, $C^k$, $H^k$, $SB^k$ і $B^k$ – дезінформатор, спамер, крекер, хакер, спам-бот і бот-зломщик відповідно) на основі восьми НП $P_1^k$, $P_2^k$, $P_3^k$, $P_4^k$, $P_5^k$, $P_6^k$, $P_7^k$ і $P_8^k$ ($T\log^k$, $N\log^k$, $TS\log^k$, $I^k$, $CPU^k$, $NEF^k$, $NEr^k$ і $RT\,\mathrm{Pr}/F^k$ – час входу в систему, частота запитів на вхід у систему, час затра-

чений на вхід в систему, інтенсивність дій, процесорний час/завантаженість процесора, кількість виконуваних файлів, кількість збоїв та помилок і час виконання процесу/файлу відповідно) та семи чітких параметрів $SP_1^k$, $SP_2^k$, $SP_3^k$, $SP_4^k$, $SP_5^k$, $SP_6^k$ і $SP_7^k$ *(*$UID^k$, $AtEF^k$, $U\,\mathrm{Pr}^k$, $TrFin^k$, $ModF^k$, $TrFout^k$ і $KS^k$ – ім'я користувача при вході, тип використовуваних файлів при атаці, невластиві процеси, передача файлу в систему, зміна файлів, копіювання/передача фалів з системи і натиснення клавіш відповідно) [5].

**Етап 3 – формування еталонів НП.** Цей етап направлений на отримання еталонних величин, необхідних для виміру поточних значень контрольованих параметрів. На основі ВхД, сгенерованих на етапі 2, формуємо відповідні значення еталонів лінгвістичних змінних для всіх $T_{ij}^e = \bigcup_{f=1}^{r} T_{ij}^{ef}$ з використанням вибраного методу формування ФН, наприклад, $\{T_{T\log}^{ef}, T_{N\log}^{ef}, T_{TS\log}^{ef}, T_I^{ef}, T_{CPU}^{ef}, \ldots\}$ [6]. Так, для CPU [5] отримаємо еталоні значення, які можна представити у вигляді лінгвістичних термів $T_{CPU}^{e} = \bigcup_{i=1}^{3} T_{CPU}^{ei} = \{T_{CPU}^{e1}, T_{CPU}^{e2}, T_{CPU}^{e3}\} = \{\underset{\sim}{\mathrm{H}}^e, \underset{\sim}{\mathrm{C}}^e, \underset{\sim}{\mathrm{B}}^e\}$ та відобразити за допомогою процедури візуалізації.

**Етап 4 – формування множини ЕП.** Етап орієнтований на створення наборів чітких та нечітких ЕП, що використовуються для виявлення порушників в ІКС на основі порівняння еталонних та поточних значень. На основі множин лінгвістичних ідентифікаторів $\boldsymbol{LI} = \bigcup_{i=1}^{d} LI_i$ [7] і наборів логіко-лінгвістичних зв'язок $\boldsymbol{LC} = \bigcup_{i=1}^{n} (\bigcup_{j=1}^{c_n} LC_{ij})$ [7] формується множина альтернатив $E\mathrm{R}_{ij}^k$ $(\mathrm{i} = \overline{1,n};\ \mathrm{k} = \overline{1,d};\ \mathrm{j} = \overline{1,r_n}$, де $n$ і $r_n$ – відповідно кількість категорій порушників правил для виявлення їх $i$-ої категорії, а $d$ – кількість альтернативних варіантів для формування одного правила). Наприклад, для першої категорії порушника і першого правила $d = 5$ отримаємо $\bigcup_{k=1}^{d} ER_{11}^k = \{ER_{11}^1, ER_{11}^2, \ldots, ER_{11}^5\}$. Формування правил здійснюється на основі множини альтернатив за допомогою процедури їх вибору, яка базується на одному з МВКВ, генеруючи таким чином набори ЕП [7], наприклад,

$$\mathrm{ER}_3 = \{\mathrm{ER}_{31} = (\mathrm{t_I} \cong B, \mathrm{t_{CPU}} \cong B, \mathrm{t_{NEr}} \cong B, \mathrm{t_{RTPr/F}} \cong ДМ) \to B, \mathrm{ER}_{32} = (\mathrm{t_I} \cong B, \mathrm{t_{CPU}} \cong B, \mathrm{t_{NEr}} \cong B, \mathrm{t_{RTPr/F}} \cong M) \to БВН\}.$$

У другій фазі обробляються НП, що використовуються для виявлення ПІБ та віднесення його до однієї з визначених категорій. Якщо результат роботи другої фази є позитивним, тобто виявлені ознаки порушення ІБ, запускається третя фаза методу. Фаза роботи з чіткими параметрами має уточнююче значення, оскільки процес ідентифікації НАС значно ефективніший на основі чітких параметрів на відміну від процесу виявлення факту порушення, який доцільно проводити на основі НЛ. На другій та третій фазі виділяються етапи 5-8.

**Етап 5 – формування зв'язки категорії порушника з параметрами.** Під час виконання другої фази здійснюється обробка НП. При цьому формуються зв'язки конкретного типу ПІБ з параметрами, що необхідні для його виявлення. Наприклад, при $n$=6 і $m$=8 в $k$-ому вузлі для ідентифікаторів порушника $I_1^k$, $I_2^k$, $I_3^k$, $I_4^k$, $I_5^k$ і $I_6^k$ створюються зв'язки з параметрами $P_{n_1}^k = P_{n_3}^k = P_{n_4}^k = (P_1^k, P_2^k, P_3^k, P_5^k, P_6^k, P_7^k, P_8^k)$, $P_{n_2}^k = P_{n_5}^k = (P_4^k, P_5^k, P_7^k, P_8^k)$ і $P_{n_6}^k = (P_1^k, P_2^k, P_3^k, P_4^k, P_5^k, P_6^k, P_7^k, P_8^k)$, тобто $\mathrm{D}^k = C^k = H^k \to \{T\log^k, N\log^k, TS\log^k, CPU^k, NEF^k, NEr^k, RT\,\mathrm{Pr}/F^k\}$, $\mathrm{S}^k = \mathrm{SB}^k \to \{I^k, CPU^k, NEr^k, RT\,\mathrm{Pr}/F^k\}$ і $\mathrm{B}^k \to \{T\log^k, N\log^k, TS\log^k, I^k, CPU^k, NEF^k, NEr^k, RT\,\mathrm{Pr}/F^k\}$, $(\mathrm{k} = \overline{1,l})$, де $l$ – кількість вузлів ІКС. Після переходу до третьої фази виконується обробка чітких параметрів для формування зв'язки конкретного типу порушника з чіткими параметрами, що необхідні для його ідентифікації. Наприклад, при $n$=6 і $m$=7 в $k$-ому вузлі з ідентифікаторами порушника $I_1^k$, $I_2^k$, $I_3^k$, $I_4^k$, $I_5^k$ і $I_6^k$ створюються зв'язки з чіткими параметрами $SP_{n_1}^k = SP_{n_2}^k = SP_{n_3}^k = SP_{n_4}^k = SP_{n_5}^k = SP_{n_6}^k = (SP_1^k, SP_2^k, SP_3^k, SP_5^k, SP_6^k, SP_7^k)$, тобто $\mathrm{D}^k = S^k = C^k = H^k = SB^k = B^k \to \{UID^k, AtEF^k, U\,\mathrm{Pr}^k, TrFin^k, ModF^k, TrFout^k, KS^k\}$.

**Етап 6 – формування та фазифікація параметрів.** Робота цього етапу також проходить у

два кроки: спочатку з НП, а потім з чіткими. По закінченню процедури формування зв'язок $I_i^k \to P_{n_i}^k$ відбувається перетворення множини поточних значень параметрів, (що фіксуються протягом певного проміжку часу) в нечітке число і таким чином отримаємо $m$ нечітких чисел $\underset{\sim}{t}_i^k$ ($i = \overline{1,m}$) (по кожному параметру), пов'язаних з відповідним $I_i^k$. Наприклад, при $m$=6 матимемо:

$\underset{\sim}{\mathrm{t}}_1^{\mathrm{k}} = \underset{\sim}{\mathrm{t}}_{T\log}^{\mathrm{k}}$, $\underset{\sim}{\mathrm{t}}_2^{\mathrm{k}} = \underset{\sim}{\mathrm{t}}_{N\log}^{\mathrm{k}}$, $\underset{\sim}{\mathrm{t}}_3^{\mathrm{k}} = \underset{\sim}{\mathrm{t}}_{TS\log}^{\mathrm{k}}$, $\underset{\sim}{\mathrm{t}}_4^{\mathrm{k}} = \underset{\sim}{\mathrm{t}}_I^{\mathrm{k}}$,

$\underset{\sim}{\mathrm{t}}_5^{\mathrm{k}} = \underset{\sim}{\mathrm{t}}_{CPU}^{\mathrm{k}}$, $\underset{\sim}{\mathrm{t}}_6^{\mathrm{k}} = \underset{\sim}{\mathrm{t}}_{NEF}^{\mathrm{k}}$, $\underset{\sim}{\mathrm{t}}_7^{\mathrm{k}} = \underset{\sim}{\mathrm{t}}_{NEr}^{\mathrm{k}}$ і $\underset{\sim}{\mathrm{t}}_8^{\mathrm{k}} = \underset{\sim}{\mathrm{t}}_{RT\,\mathrm{Pr}/F}^{\mathrm{k}}$.

Під час третьої фази по закінченню процедури формування зв'язок $I_i^k \to SP_{n_i}^k$ визначаються поточні значення чітких параметрів $SP_i^k$ на момент переходу до третьої фази, які передаються з кожного вузла системи на відповідні кожному параметру модулі логічної арифметики.

**Етап 7 – обробка і формування кортежів параметрів.** Етап орієнтований на визначення значення кожного з параметрів (нечітких та чітких) для усієї системи загалом і формування їх в один кортеж. Сформовані $\underset{\sim}{\mathrm{t}}_{\mathrm{i}}^{\mathrm{k}}$ ($\mathrm{i} = \overline{1,n}, \mathrm{k} = \overline{1,l}$) паралельно (відповідно до кожного параметру) з використанням обраного методу НА обробляються для отримання сумарних показників, що позначені – $\sum \underset{\sim}{t}^k$ і які характеризують величину контрольованих параметрів на всіх вузлах ІКС. На цьому етапі використовується один з можливих методів реалізації операцій НА відповідно до заданих користувачем критеріїв (для запропонованого методу найбільш доцільно використовувати метод ЛАЛМ). Якщо процес виявлення порушника здійснюється тільки в одному вузлі ІКС, то жодних логічних та арифметичних операцій на ньому не виконується і не створюються сумарні значення змінних. Отримані сумарні показники записуються за кожним параметром у кортеж, який позначено – $< \sum \underset{\sim}{t}_i >$. Фаза роботи з чіткими параметрами містить їх обробку і обчислення результуючого (сумарного) значення для усієї ІКС, яке позначено – $\sum SP_i^k$. Обчислення відбувається за правилами звичайної логіки. Якщо значення чіткого параметру хоча б на одному з вузлів дорівнює «1», то сумарне значення також рівне «1». Якщо процес виявлення ПІБ здійснюється тільки на одному вузлі ІКС, то жодних логічних та арифметичних операцій на ньому не виконується і не створюються сумарні значення змінних. Отримані дані формуються в кортеж позначений як $< \sum SP_i >$.

**Етап 8 – формування результату.** Етап орієнтований на прийняття рішення щодо фіксації порушення ІБ в ІКС, тобто визначення факту порушення та ідентифікація НАС за однією із запропонованих категорій (дезінформатор, спамер, крекер, хакер, спам-бот, бот-зломщик). На основі сформованого кортежу $< \sum \underset{\sim}{t}_i >$ з використанням множини правил $ER_i$ ($\mathrm{i} = \overline{1,n}$) за допомогою логіко-лінгвістичних зв'язок $LI_i$ ($\mathrm{i} = \overline{1,d}$) виконується порівняння ФН НП зі значеннями ЕП за допомогою методу АРВ (або відстані Хеммінга) [2], тобто виявлення можливого порушника і ідентифікація його типу.

Іншими словами, кожній категорії НАС $I_i^k$ присвоюється логічний ідентифікатор *LI (Н, БНВ, С, БВН, В, К)* [7]. Отриманий результат може відображатися як в лінгвістичній, так і в графічній формі у вигляді нечіткого числа, інтегрованого з еталонними значеннями лінгвістичних змінних. Саме на цьому етапі формується проміжний результат, що засвідчує факт порушення ІБ в ІКС і далі реалізується 3-тя фаза методу, де здійснюється робота з чіткими параметрами на етапах 5-8. У результаті на основі згенерованого кортежу $< \sum SP_i >$ з використанням множини правил $ESR_i$ ($\mathrm{i} = \overline{1,n}$), відповідних певному типу $I_i^k$ виконується ідентифікація типу можливого порушника із визначеної множини. Слід також зазначити, що кількість як ідентифікаторів (тобто категорій) НАС, так і параметрів, за якими можна виявити факт порушення ІБ може бути за рішенням експерта змінена у процесі роботи системи, розробленої на основі даного метода.

**Висновки.** Таким чином, у цій роботі було вперше розроблено метод ВІП в ІКС, який, за рахунок використання математичного апарату НЛ, дає можливість виявити ПІБ у НВСС і ідентифікувати відповідно до виділених категорій. Метод містить 3 фази та 8 етапів, для реалізації яких ВхД є мережеві та/або хостові параметри та ідентифікатори порушника (можливі категорії), а на виході формується повідомлення про фіксацію факту по-

рушника та результат процедури категоризації порушника. Використання цього методу дасть можливість підвищити ефективність сучасних засобів виявлення та попередження вторгнень в ІКС за рахунок розширення їх функціональності.

## ЛІТЕРАТУРА


[1]. Корт С.С. Структура систем обнаружения нарушителя (СОН)[Електронній ресурс]: стаття / С. С. Корт. – Режим доступу: http://www.ssl.stu.neva.ru/sam/.

[2]. КорченкоА. Г. Построение систем защиты информации на нечетких множествах [Текст] : Теория и практические решения / А. Г. Корченко. — К. : МК-Пресс, 2006. — 320 с.

[3]. Волянська В. В. Система виявленняаномалій на основінечітких моделей [Текст] / В. В. Волянська, А. О. Корченко, Є. В. Пациpa // Зб. наук.пр. Інституту проблем моделювання в енергетиці НАН Україниім. Г. Є Пухова. — Львів : ПП «Системи, технології, інформаційніпослуги», 2007. — [Спец. випуск]. — Т.2. — С. 56–60.

[4]. Корченко О. Г. Системи захистуі нформації [Текст] :Монографія / О. Г. Корченко. — К. : НАУ, 2004. — 264 с.

[5]. Гізун А.І. Основні параметри для ідентифікації порушника інформаційної безпеки / А.І. Гізун, В.В. Волянська, В.О. Риндюк, С.О. Гнатюк // Захист інформації. – 2013. –№1 (58). – С.66-75.

[6]. Волянська В.В. Моделі еталонів лінгвістичних змінних для систем виявлення та ідентифікації порушника інформаційної безпеки// В.В. Волянська, А.І. Гізун, В.О. Гнатюк / Безпека інформації. –№1 (19). – 2013. – С. 13-21.

[7]. Гізун А.І. Евристичні правила на основі логіколінвистичних зв'язок для виявлення та ідентифікації порушника інформаційної безпеки / А.І. Гізун, В.В. Волянська, О.В. Гавриленко, А.О. Корченко // Захист інформації. – 2013. –№3 (60). – С.251-257.

[8]. Горніцька Д.А. Визначення коефіцієнтів важливості для експертного оцінювання у галузі інформаційної безпеки / Д.А. Горніцька, В.В Волянська, А.О. Корченко // Захист інформації. — 2012. — №1 (54). — С. 108-121.


## REFERENCES


[1]. Kort S.S. The structure of intruder detection systems [Electronic resource]: abstract / S.S. Kort. – Modeofaccess: http://www.ssl.stu.neva.ru/sam/

[2]. Korchenko A.G. Development of the security systems on fuzzy sets. Theory and practical solutions / A.G. Korchenko, K.: "MK-Press", 2006, 320 P.

[3]. Korchenko A.O. Anomaly detection system based on fuzzy models / A.O. Korchenko, Ye.V. Patsira, V.V. Volyanska // Modern trainer and educational complexesand systems. – L.: Institute for Modelling in Energy NAS of Ukraine named. G.Ye. Pukhov, 2007, T.2., P. 56–60.

[4]. Korchenko A.G. System of information security / A.G. Korchenko, K.: NAU, 2004, 264 P.

[5]. Gizun A.I. The main parameters to identify the intruder of information security / A.I. Gizun, V.V. Volyanska, V.O. Ryndyuk, S.O. Gnatyuk // Ukrainian Information Security Research Journal. – 2013. –№1 (58). – P.66-75.

[6]. VolyanskaV.V. Models of standards of linguistic variables for detection and identification the intruder of information security// V.V. Volyanska,A.I. Gizun, V.O. Gnatyuk / Ukrainian Scientific Journal of Information Security. –№1 (19). – 2013. –P. 13-21.

[7]. Gizun A.I. Heuristic rules based on logic-linguistic connection for information security intruder`s detection and identification / A.I. Gizun, V.V. Volyanska, O.V. Gavrylenko, A.O. Korchenko // Ukrainian Information Security Research Journal. – 2013. –№3 (60). – P.251-257.

[8]. Gornits'kaD.A. Coefficients determining of importance for the expert assessment in information security / D.A. Gornits'ka, V.V. Volyanska, A.O. Korchenko // Information Security Research Journal. — 2012. — №1 (54) . — P. 108-121


## МЕТОД ВЫЯВЛЕНИЯ И ИДЕНТИФИКАЦИИ НАРУШИТЕЛЯ В ИНФОРМАЦИОННО-КОМУНИКАЦИОННЫХ СИСТЕМАХ


Обеспечение безопасности государственных информационных ресурсов неразрывно связано с выявлением деятельности нарушителя информационной безопасности (ИБ) в информационно-коммуникационных системах (ИКС), в которых циркулирует информация с ограниченным доступом. Недостатком современных систем обнаружения нарушителя ИБ, построенных на эвристических правилах (ЭП) в том, что они в основном ориентированы на использование таких математических моделей, которые требуют много времени на подготовку статистических данных. Математические модели, основанные на экспертных подходах, в этом отношении являются более эффективными. Предлагается метод, позволяющий на основе суждений эксперта в нечетких условиях решить задачу обнаружения и идентификации нарушителя (ОИН) в ИКС. В методе используются элементы нечеткой логики для предварительного принятия решения о нарушении и идентификации личности нарушителя, а также базис

обычной четкой логики, обеспечивает уточняющую информацию. Метод включает этапы: формирование коэффициентов важности, множеств категорий нарушителя и параметров, эталонов нечетких параметров, множества ЭП, связь категории нарушителя с параметрами; формирование и фаззификации параметров, обработки и формирования кортежей параметров; формирование результата. Работа метода организована в 3 фазы: подготовительная; работа с нечеткими параметрами; работа с четкими параметрами. Основываясь на этом методе может быть синтезирована система ОИН, базируемая на ЭП и характеризуемая высокой эффективностью работы в условиях нечеткости.
**Ключевые слова:** системы обнаружения нарушителя, нарушитель информационной безопасности, идентификация, выявление аномалий в информационно-коммуникационных системах, метод, нечеткая логика, базовая модель идентификации нарушителя, логико-лингвистическая связка, эвристические правила, экспертная оценка.

## METHOD OF INTRUDER DETECTION AND IDENTIFICATION IN INFORMATION & COMMUNICATION SYSTEMS

The providing of state information resources security is inextricably connected with information security intruder`s activity in information & communication systems where restricted data is circulating. The modern intruder detection systems, based on heuristic principle of information security violation detection, have a disadvantage because these are basically oriented on mathematical models which require much time to prepare statistic data. Mathematical models based on expert approach are more effective in this way. The method proposed in paper allows to solve the problem of intruder detection and identifying in information & communication systems and networks, which are weakly-formalized fuzzy environment. In the method elements of fuzzy logic are used to the previous decision of the violation & the intruder identification and precise basis of conventional logic that provides clarifying identification. The method consists of such stages: selection of the method for determining the importance of factors, the formation of categories sets of intruder and parameters, forming standards of fuzzy parameters, forming the set of heuristic rules, forming connections of intruder category with parameters, phasing of fuzzy parameters and definition clear parameters, processing and forming of parameters corteges, results formation. The method`s work is organized in three phases: preparation, work with fuzzy parameters and work with clear parameters. On the basis of this method can be synthesized heuristic type intruder detection & identification system with high performance in fuzzy terms by the use of expert methods.
**Key words:** intruder detection system, information security intruder, identification, anomaly detection in information & communication system, method, fuzzy logic, basic model of intruder identification, logic-linguistic connection, heuristic rules, expert estimation.

**Корченко Анна Олександрівна**, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: annakor@ukr.net
**Корченко Анна Александровна**, кандидат технических наук, доцент кафедры безопасности информационных технологий Национального авиационного университета.
**Anna Korchenko** PhD in Eng., Associate Professor of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).

**Казмирчук Светлана Владимировна**, кандидат технических наук, доцент кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: sv902@mail.ru
**Казмірчук Світлана Володимирівна**, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
**Kazmirchuk Svitlana**, PhD in Eng., Associate Professor of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).

**Гізун Андрій Іванович**, асистент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: andriy.gizun@gmail.com
**Гизун Андрей Иванович**, асистент кафедры безопасности информационных технологий Национального авиационного университета.
**Gizun Andriy,** Assistant in Academic Department of IT-security, National Aviation University.

**Волянська Владислава Вікторівна**, IT-менеджер Apogeum Sp. z o.o. Poland.
E-mail: volyanska.vladyslava@gmail.com
**Волянская Владислава Викторовна**, ИТ-менеджер Apogeum Sp. Z o.o. Poland.
**VolyanskaVladyslava**, IT-manager in Apogeum Sp. z o.o. Poland.

**Гнатюк Сергій Олександрович**, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: s.gnatyuk@nau.edu.ua
**Гнатюк Сергей Александрович**, кандидат технических наук, доцент кафедры безопасности информационных технологий Национального авиационного университета.
**Sergiy Gnatyuk**, PhD, Associate Professor in Academic Department of IT-security, National Aviation University.