pared from cryptographic strength providing point of view.
Index terms: permutation, variable length blocks, open message, ciphertext, pseudorandom numbers generator.

Лужецький Володимир Андрійович, доктор технічних наук, професор, завідувач кафедри захисту інформації, Вінницький національний технічний університет.
E-mail: lva_zi@mail.ru.
Лужецкий Владимир Андреевич, доктор технических наук, профессор, заведующий кафедрой защиты информации, Винницкий национальный технический университет.
Luzhetsky Volodymyr, Doctor of Technical Sciences, Professor, Head of Information Security Academic Departmant, Vinnytsia National Technical University.

Горбенко Іван Сергійович, аспірант кафедри захисту інформації, Вінницький національний технічний університет.
E-mail: milyaga89@gmail.com.
Горбенко Иван Сергеевич, аспирант кафедры защиты информации, Винницкий национальный технический университет.
Gorbenko Ivan, postgraduate student Information Security Academic Departmant, Vinnytsia National Technical University.

УДК 004.056.53:004.492.3 (045)

МЕТОД ВИЯВЛЕННЯ ІНЦИДЕНТІВ/ПОТЕНЦІЙНИХ КРИЗОВИХ СИТУАЦІЙ

Микола Карпінський, Анна Корченко, Андрій Гізун

Розвиток інформаційних технологій призвів до збільшення залежності людського суспільства від них і різкого зростання інцидентів інформаційної безпеки, що за умов відсутності контролю за ними можуть спричиняти кризові ситуації. Чим вищий рівень критичності інциденту/потенційної кризової ситуації, тим серйозніші збитки він здатен завдати і тому вимагає значно серйознішого захисту. Одним з основних аспектів, який визначає ефективність захисту, є автоматизація і своєчасність виявлення та ідентифікації інцидентів. В роботі запропонований метод виявлення інцидентів/потенційних кризових ситуацій, що базується на застосуванні теорії нечітких множин та експертних підходів. Оскільки процеси в інформаційних системах характеризуються певним рівнем невизначеності та випадковості і носять нечіткий характер, то такий метод може бути використаний для реалізації задач захисту інформації. Складається метод з 6 етапів: формування множин інцидентів/потенційних кризових ситуацій та ідентифікуючих параметрів; формування зв'язки інцидент – набір нечітких ідентифікуючих параметрів; формування еталонів нечітких параметрів; формування наборів евристичних правил для виявлення та ідентифікації інцидентів; фазифікації параметрів, що моніторяться для виявлення інциденту; обробки параметрів та формування результату. Запропонований метод може застосовуватися окрема або в комплексі з методом оцінки рівня критичності ситуації, що склалася внаслідок впливу інциденту/потенційної кризової ситуації.
***Ключові слова**: кризова ситуація, інцидент, рівень критичності кризової ситуації, експертні методи, теорія нечітких множин, виявлення та ідентифікація кризових ситуацій, інтегрована модель.*

Враховуючи стрімкий розвиток інформаційних технологій, що впливає як на захисні механізми так і на засоби для проведення інформаційних атак, набір можливих інцидентів/потенційних кризових ситуацій (ІПКС) значно збільшується. Безперервно зростає кількість загроз інформаційній безпеці, проводяться нові кібератаки на інформаційні ресурси (ІР), що ускладнює реалізацію ефективного захисту. Досягнення максимального ефекту захищеності ІР можливе за умови обізнаності щодо можливих ІПКС, що створює передумови для підбору та застосування найбільш адекватних заходів та засобів захисту. Крім того, задачі прийняття рішень в умовах КС потребують значних часових та виробничих ресурсів, а також встановлення додаткових вимоги до особи, що приймає рішення, з точки зору швидкості її реакції та вміння оцінити поточне становище. Дана задача ускладнюється тим, що атаки на ІР здійснюються в реальних умовах, тобто з великим показником випадковості та непередбачуваності. Виходячи з цього дуже складно оперувати статистичними даними, які використовуються в класичних методах та засобах управління КС. Дану проблему може вирішити застосування методів та математичного апарату нечіткої логіки, ефективність застосування яких для вирішення задач, пов'язаних з забезпеченням інформаційної безпеки, показана в роботі [1]. Тому розробка методу виявлення ІПКС є актуальною задачею.

Системи захисту інформації, засновані на теорії нечітких множин, дозволяють забезпечувати захищеність ІР в ІС незважаючи на високий ступінь невизначеності інформаційних процесів. Однак вони на сьогодні є не чисельними і вузькоспеціалізованими. Відомі роботи в яких описані методи, системи та підходи виявлення та ідентифікації порушника інформаційної безпеки [2,3], аномального стану в інформаційних системах (ІС), породженого впливом кібератак [4]. Стосовно методів та систем управління КС з подібним принципом функціонування слід відмітити роботи, в яких розроблена модель представлення ІПКС [5], яка заснована на підходах описаних в [6,7], визначені основні ІПКС, параметри для їх ідентифікації [8], запропонована процедури побудови нечітких еталонів ідентифікуючих параметрів [5] та евристичних правил для виявлення ІПКС [9]. Крім того в роботі [10] описаний метод оцінки рівня критичності ситуації, спричиненої ІПКС.

Оскільки класичні системи управління КС не можуть ефективно застосовуватися в умовах нечіткості, то метою роботи є автоматизація та підвищення ефективності відомих систем управління КС за рахунок розробки методу виявлення ІПКС, що ґрунтуються на застосуванні методів нечіткої логіки та експертних підходів дає принципову можливість виявити та ідентифікувати ІПКС у певному середовищі в нечітких умовах.

Запропонований метод використовується для прийняття рішення щодо факту наявності ІПКС. Він може застосовуватися в комплексі з методом оцінки критичності ситуації [10] або окремо. Вхідними даними методу виявлення ІПКС є параметри середовища, які підлягають моніторингу та ідентифікатори ІПКС, на виході формується повідомлення про фіксацію факту інциденту з уточненням можливості його настання. Схематичне відображення методу наведене на рис. 1, де застосовуються методи: лінгвістичних термів з використанням статистичних даних (МЛТС) – для побудови еталонних значень параметрів; лінійної апроксимації по локальним максимумам (ЛАЛМ) – для виконання нечітких математичних операцій; узагальнена відстань Хемінга (УВХ) – для порівняння поточних і еталонних значень параметрів. Також використовується експертні методи оцінювання та ранжування, а саме метод середніх рангів (СР). Запропонований метод складається з 6 етапів:

Етап 1 – формування множин ІПКС та ідентифікуючих параметрів. Етап направлений на визначення множин ІПКС та параметрів для їх ідентифікації. На основі аналізу середовища ІС формуються ідентифікатори ІПКС з множини $\mathbf{IKS} = \{\bigcup_{i=1}^{n} \mathbf{IKS_i}\}$, $(i = \overline{1,n})$, де n – загальна кількість ІПКС, а також множина параметрів $\mathbf{P} = \{\bigcup_{j=1}^{m} P_j\}$, $(j = \overline{1,m})$ [5], поточні значення яких з певною періодичністю заносяться в регістри системи виявлення ІПКС. Тобто фіксуються IKS_i та P_j [5,7], що є вхідними даними даного методу та системи виявлення ІПКС. Наприклад, при $n = 5$ та $m = 13$ система здатна виявити такі потенційні КС, які мають ідентифікатори $IKS_1 = ZL$, $IKS_2 = SP$, $IKS_3 = DD$, $IKS_4 = VA$, $IKS_5 = ZK$ з іменами «Злом ІС», «Спам», «Відмова в обслуговуванні», «Вірусна атака» та «Вихід з ладу ІС через вплив кліматичних умов» відповідно) на основі 13 нечітких параметрів P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9, P_{10}, P_{11}, P_{12}, P_{13} (де $P_1 = Tlog$, $P_2 = Nlog$, $P_3 = CPU$, $P_4 = MU$, $P_5 = NEr$, $P_6 = RTPr$, $P_7 = CNCh$, $P_8 = NCC$, $P_9 = DbR$, $P_{10} = STF$, $P_{11} = T$, $P_{12} = H$, $P_{13} = D$ – відповідно ідентифікатори таких параметрів як «Час входу в систему», «Частота запитів на вхід у систему», «Завантаженість процесора», «Завантаженість оперативної пам'яті», «Кількість збоїв та помилок», «Час виконання процесу», «Завантаженість мереженого каналу», «Кількість одночасних підключень», «Затримка між запитами від одного джерела», «Розмір тимчасових файлів», «Температура в серверній кімнаті», «Вологість повітря в серверній кімнаті», «Концентрація пилу в серверній кімнаті») [8].

Етап 2 – формування зв'язки ІПКС з параметрами. На цьому етапі формуються зв'язки конкретного типу ІПКС з параметрами, що необхідні для його виявлення. Вхідними даними на даному етапі є ідентифікатори інцидентів і нечіткі параметри, занесені в регістри системи виявлення ІПКС на попередньому етапі. Формується n підмножин параметрів $\mathbf{P_i} \subseteq \mathbf{P}$, кожна з яких містить k_i елементів, а на їх основі створюються зв'язки «ІПКС» → «ідентифікуючий параметр», тобто $\mathbf{IKS_i} \to \mathbf{P_i}$. Наприклад, при $n = 5$ та $k_1 = k_3 = 6$, $k_2 = k_4 = 5$, $k_5 = 3$ будуть сформовані такі зв'язки: $IKS_1 = ZL \to \{Tlog, Nlog, CPU, MU, NEr, RTPr\}$, $IKS_2 = SP \to \{CPU, MU, NEr, RTPr, CNCh\}$, $IKS_3 = DD \to \{CPU, MU, NEr, CNCh, NCC, DbR\}$, $IKS_4 = VA \to \{CPU, MU, NEr, CNCh, STF\}$, $IKS_5 = ZK \to \{T, H, D\}$.

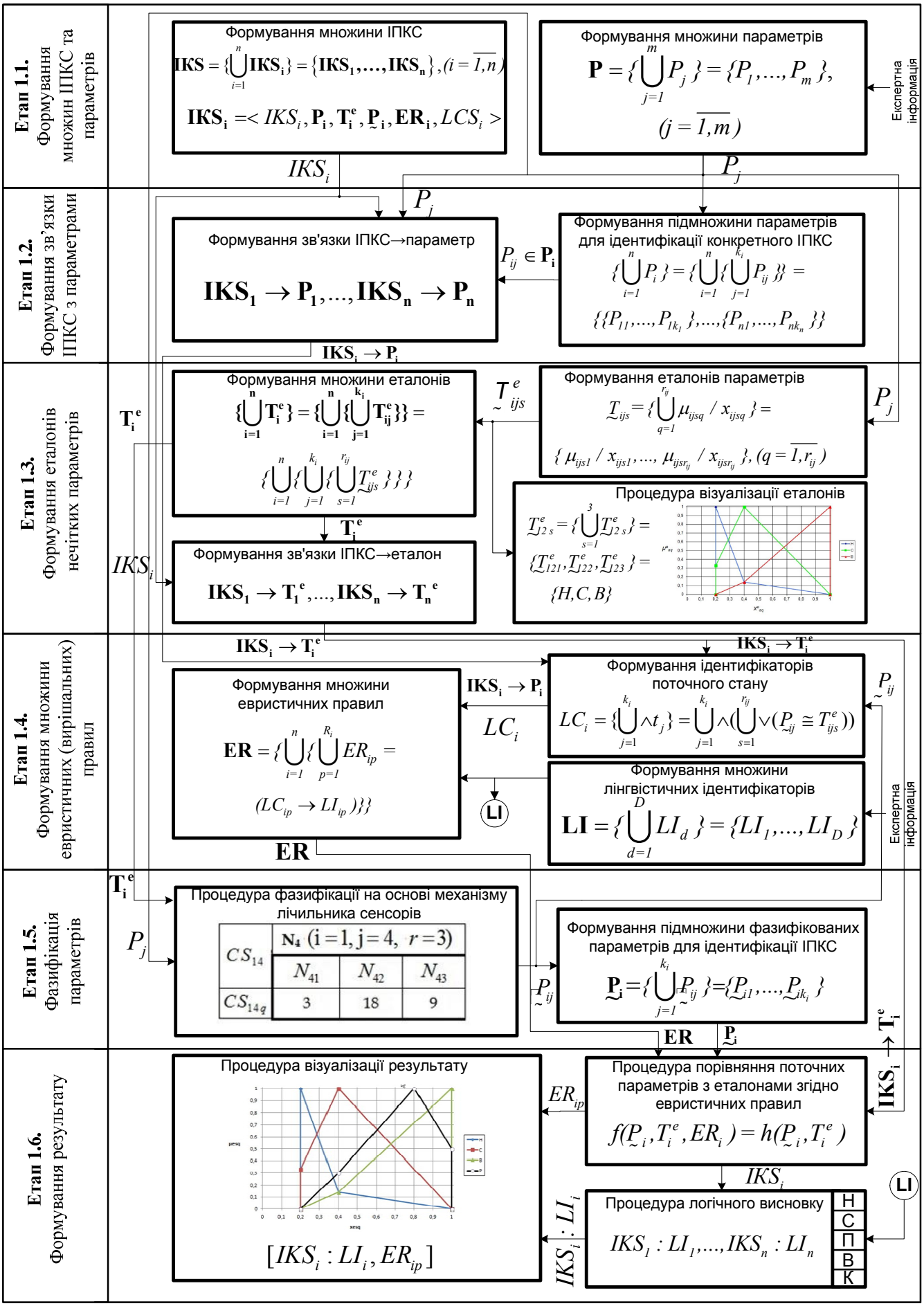

Рис. 1. Схема відображення методу виявлення ІПКС

Етап 3 – формування еталонів нечітких параметрів. На цьому етапі отримаємо еталонні величини, необхідні для виміру поточних значень контрольованих параметрів. Вони визначають множину еталонів $\{\bigcup_{i=1}^{n} \mathbf{T_i^e}\} = \{\mathbf{T_1^e}, \ldots, \mathbf{T_n^e}\}$, $(i = \overline{1,n})$ необхідних для виявлення конкретного ІПКС. На основі вхідних даних (див. етап 1), отриманих шляхом використання експертних методів, формуємо відповідні значення еталонів лінгвістичних змінних для всіх $\mathbf{T_{ij}^e} = \{\bigcup_{s=1}^{r_{ij}} T_{ijs}^e\}$ з використанням вибраного методу формування функцій належності, наприклад, при $IKS_1 = ZL$ матимемо $\mathbf{T_{ZL}^e} = \{\bigcup_{j=1}^{k_{ZL}} T_{ZLj}^e\} = \{T_{ZLTlog}^e, \ ..., \ T_{ZLRTPr}^e\}$. Так, для CPU [8] отримаємо еталоні значення $T_{CPU}^e = \{\bigcup_{s=1}^{3} T_{CPUs}^e\} = \{T_{CPU1}^e, \ T_{CPU2}^e, \ T_{CPU3}^e\} = \{\underset{\sim}{H}^e, \underset{\sim}{C}^e, \underset{\sim}{B}^e\}$, які можна представити у вигляді лінгвістичних термів $\underset{\sim}{H}^e, \underset{\sim}{C}^e, \underset{\sim}{B}^e$ за допомогою процедури візуалізації [5]. Процедура формування еталонів здійснюється за допомогою МЛТС, формалізованого за аналогією з [11]. Крім того, аналогічно до етапу 2 створюються зв'язки «ІПКС» → «еталон ідентифікуючого параметра», $\mathbf{IKS_i} \rightarrow \mathbf{T_i^e}$.

Етап 4 – формування множини евристичних (вирішальних) правил (ЕП). Створення наборів ЕП, що використовуються для виявлення ІПКС на основі зіставлення еталонних $\underset{\sim ijs}{T^e}$ та поточних значень параметрів з множини $\underset{\sim}{\mathbf{P_i}}$ $(i = \overline{1,n})$ за допомогою набору ідентифікаторів поточного стану LC, що є унікальним для кожного ІПКС. На основі цього створюємо набір $\mathbf{ER} = \{\bigcup_{i=1}^{n} ER_i\}$, що містить ЕП виявлення та ідентифікації всіх ІПКС. Для їх формування використовуються лінгвістичні ідентифікатори LI_i можливості реалізації ІПКС, необхідні для відображення судження експерта в лінгвістичній формі. Далі сформуємо множину альтернатив ER_{ip}^d $(i = \overline{1,n}; \ d = \overline{1,D}; \ p = \overline{1,R_n}$, де n – кількість категорій ІПКС, R_n – кількість правил для виявлення i-ї категорії порушника, а D – кількість альтернативних варіантів для формування одного правила). Наприклад, для першої категорії порушника і першого правила отримаємо $\mathbf{ER_{11}} = \{\bigcup_{d=1}^{D} ER_{11}^d\} = \{ER_{11}^1, \ ..., \ ER_{11}^D\}$. Формування правил здійснюється на основі множини альтернатив за допомогою процедури їх вибору, яка базується на методі СР. Так, 1-е правило для виявлення $\mathbf{IKS_4 = VA}$ (вірусна атака) матиме вигляд: $ER_{41} = \{(t_{CPU} \cong H, \ t_{CNCh} \cong H, \ t_{SIF} \cong M, \ t_{MU} \cong H, \ t_{NEr} \cong M) \rightarrow H\}$. Детально процедура формування правил та приклади наборів наведені в роботі [9].

Етап 5 – фазифікація параметрів, що моніторяться з метою виявлення ІПКС. На даному етапі відбувається перетворення множини поточних значень параметрів, що фіксуються кожні t проміжки часу протягом певного періоду Т в одне нечітке число і таким чином отримаємо значення, характеризуючі поточні стани контрольованого середовища. Сформовані нечіткі показники групуються з врахування процедури створення зв'язок $\mathbf{IKS_i} \rightarrow \mathbf{P_i}$ в підмножини для виявлення окремого ІПКС з k_i елементів, тобто $\underset{\sim}{\mathbf{P_i}} = \{\bigcup_{j=1}^{k_i} \underset{\sim ij}{P}\}$, $(i = \overline{1,n})$. Саме вони використовуються на наступному кроці при виявлені інцидентів. Фазифікація здійснюється на основі механізму лічильника сенсорів [11], при чому вхідними параметрами є їх показники і нечіткі еталони лінгвістичних змінних.

Етап 6 – обробка поточних значень ідентифікуючих параметрів і формування результату. Етап спрямований на прийняття рішення щодо наявності ІПКС, що можуть загрожувати інформаційній безпеці. Сформовані на попередньому етапі нечіткі числа, які відображають поточні значення контрольованих параметрів відповідно до ІПКС, які вони визначають, а функції належності їх елементів порівнюються з еталонними значеннями за допомогою визначення УВХ. На основі цього виконується порівняння ідентифікатора поточної ситуації з ЕП з заданого набору. Погодження певним правилом ідентифікатора ситуації дає змогу зробити висновок щодо наявності передумов реалізації ІПКС і таким чином поточній ситуації присвоюється відповідний лінгвістичний ідентифікатор можливості реалізації ІПКС $IKS_i : LI_i$. Тобто фіксується факт появи ІПКС (його виявлення). Отриманий результат може відображатися в лінгвістичній

формі, у вигляді нечіткого числа або лінгвістичної змінної з зазначенням правила, яке ідентифікувало (погодило) поточну ситуацію. Наприклад, при $i = 4$ та якщо на етапі 5 були виміряні та фазифіковані наступні значення контрольованих параметрів, з яких сформовано ідентифікатор поточної ситуації у вигляді $LC_4 = (t_{CPU} \cong B,\ t_{CNCh} \cong B,\ t_{STF} \cong B,\ t_{MU} \cong B,\ t_{NEr} \cong B)$, то дана ситуація буде ідентифікована правилом ER_{4243} з набору $\mathbf{ER_4}$. В такому випадку лінгвістичний ідентифікатор можливості реалізації ІПКС згідно даного правила відповідатиме «критичному» рівню. Таким чином на виході методу отримаємо фіксацію факту виявлення ІПКС «вірусна атака» з критичною можливістю її реалізації. Після виявлення ІПКС його необхідно оцінити за встановленою процедурою, використовуючи метод оцінки критичності ситуації, який описаний в [10].

Висновки. В роботі розроблений метод виявлення ІПКС, що за рахунок обробки нечітких ідентифікуючих та оціночних параметрів, використання інтегрованої моделі представлення інциденту, моделей еталонів та евристичних правил, дозволяє виявити ІПКС в ІС. Запропонований метод заснований на базисі теорії нечітких множин та експертних підходах, за рахунок чого дає змогу забезпечити функціонування процесів управління КС в нечіткому слабоформалізованому середовищі. На основі даного методу та методу оцінки рівня критичності [10] в подальшому необхідно розробити системи виявлення ІПКС та оцінки критичності ситуації.

ЛІТЕРАТУРА

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

[2]. Корченко А.О. Метод виявлення та ідентифікації порушника в інформаційно-комунікаційних системах / А.О. Корченко, А.І. Гізун, В.В. Волянська, С.О. Гнатюк // Захист інформації. – 2013. – Т.15. – №4. – С. 387-393.

[3]. Корченко А.О. Система виявлення та ідентифікації порушника в інформаційно-комунікаційних мережах / А.О. Корченко, В.В. Волянська, А.І. Гізун // Безпека інформації. – 2013. – Т.19. – №3. – С. 158-162.

[4]. Корченко А.А. Система выявления аномального состояния в компьютерных сетях / А.А. Корченко // Безпека інформації. – 2012. – № 2 (18). – С. 80-84.

[5]. Карпінський М.П. Інтегрована модель представлення кризових ситуацій та формалізована процедура побудови еталонів ідентифікуючих параметрів / М.П. Карпінський, А.О. Корченко, А.І. Гізун // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2015. – В.1 (29). – С. 76-85.

[6]. Корченко А.Г. Системы анализа и оценивания рисков информационной безопасности / А.Г. Корченко, А.Е. Архипов, С.В. Казмирчук. – К. : Palmarium Academic Publishing, 2013. – 316 с.

[7]. Корченко А.О. Кортежная модель формирования набора базовых компонент для выявления кибератак / А.А. Корченко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2014. – В.2 (28). – С. 29-36.

[8]. Параметры прогнозирования и идентификации атак в информационно-коммуникационных системах / В. Азарсков, А. Гизун, А. Грехов, С. Скворцов // Захист інформації. – 2014. – 16, № 1. – С. 89-95.

[9]. Гізун А.І. Формалізована модель побудови евристичних правил для виявлення інцидентів / А.І. Гізун, В.О. Гнатюк, О.М. Супрун // Вісник Інженерної академії України. – 2015. – №1. – С. 110-115.

[10]. Корченко А.О. Метод оцінки рівня критичності для систем управління кризовими ситуаціями / А.О. Корченко, В.А. Козачок, А.І. Гізун // Захист інформації. – 2015.– Т.17. – №1. – С. 86-98.

[11]. Корченко А.А. Метод формирования лингвистических эталонов для систем выявления вторжений / А.А. Корченко // Захист інформації. – Т.16, №1. – 2014. – С. 5-12.

REFERENCES

[1]. Korchenko O. G. Building security systems on fuzzy sets [Text]: theory and practical solutions, K. :MK-Press, 2006, 320 p.

[2]. Korchenko A.A, Gizun A.I., Volyanska V.V, Gnatyuk S.O. Method of intruder detection and identification in information & communication systems. Ukrainian Information Security Research Journal, 2013, T. 15, №4, P.387-393.

[3]. Korchenko A.A., Gizun A.I., Volyanska V.V, System of intruder detection and identification in information & communication networks. Ukrainian Scientific Journal of Information Security, №1 (19), 2013, P. 158-162.

[4]. Korchenko A.A. System of detection of abnormal state in computer networks Ukrainian Scientific Journal of Information Security, №1 (19), 2013, P. 158-162.

[5]. Karpinkiy M.P., Korchenko A.O., Gizun A.I. Integrated model for crises presentation and formalized procedures for identifying parameters building. Legal, Normative and metrological support of information security in Ukraine, 2015, B.2 (28), P. 76-85.

[6]. Korchenko A.G, Arkhipov A.E, Kazmirchuk S.V. Systems for analysis and assessment of information

security risks, K.: Palmarium Academic Publishing, 2013, 316 p.
[7]. Korchenko A.A. Tuple model of a set of basic components to identify cyberattacks. Legal, Normative and metrological support of information security in Ukraine. - 2014 - B.2 (28). - S. 29-36..
[8]. Azarskov V., Gizun A., Grekhov A., Skvortsov S. Parameters identification and prediction of attacks in the information and communication system, Ukrainian Information Security Research Journal, 2014, T. 16, №1, P. 89- 95.
[9]. Gizun A.I., Gnatiuk V.A., Suprun O.M. Formalized model of heuristic rules for incident detection, Journal of Engineering Academy of Ukraine, 2015, №1, P. 110-115.
[10]. Korchenko A.O., Kozachok V.A., Gizun A.I. Method of criticality level assessment for crisis management sestems. Ukrainian Information Security Research Journal, 2015, T. 17, №1, P.86-98.
[11]. Korchenko A. O. Method of forming linguistic standards for intrusion detection systems. Ukrainian Information Security Research Journal, 2014, T. 16, №1, P. 5-12.

МЕТОД ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ/ПОТЕНЦИАЛЬНЫХ КРИЗИСНЫХ СИТУАЦИЙ

Развитие информационных технологий привело к увеличению зависимости человеческого общества от них и значительному росту числа инцидентов информационной безопасности, которые при условии контроля за ними могут провоцировать кризисные ситуации. Чем выше уровень критичности инцидента/потенциальной кризисной ситуации, тем серьезнее убытки он способен нанести и поэтому требует более высокой защиты. Одним из основных аспектов, который определяет эффективность защиты, является автоматизация и своевременность выявления и идентификации инцидентов. В работе предложен метод выявления инцидентов/потенциальных кризисных ситуаций, основанный на использовании теории нечетких множеств и экспертных подходов. Поскольку процессы в информационных системах характеризируются некоторым уровнем неопределенности и случайности, носят нечеткий характер, то такой метод может быть использован для реализации задач защиты информации. Состоит метод из 6 этапов: формирование множеств инцидентов/потенциальных кризисных ситуаций и идентифицирующих параметров; формирования связки инцидент – набор нечетких идентифицирующих параметров; формирования эталонов нечетких параметров; формирование наборов эвристических правил для выявления и идентификации инцидентов; фазификация параметров, которые мониторятся для выявления инцидента; обработка параметров и формирование результата. Предложенный метод может применяться отдельно или в комплексе с методом оценки уровня критичности ситуации, сложившейся в результате воздействия инцидента/потенциальной кризисной ситуации.

Ключевые слова: кризисная ситуация, инцидент, уровень критичности кризисной ситуации, экспертные методы, теория нечетких множеств, обнаружение и идентификация кризисных ситуаций, интегрированная модель.

METHOD FOR INCIDENT/POTENTIAL CRISES DETECTION

The information technology development with increasing dependence of human society from them is also the danger of a sharp increase in information security incidents in the absence of control over them can cause crises. The higher the level of incident/potential crisis criticality causes the serious damage and it requires a much more serious security. Major aspects that determines the security effectiveness is the automation, timely detection and identification of incidents. In this paper method of incidents/potential crisis identifying based on the application of fuzzy sets theory and expert approaches was proposed. Thus the method can be used in conditions of weakly-formalized environment, like information and communication systems or networks. This method consists of 6 phases: forming sets of incidents/potential crisis and identifying parameters; forming ties incident – identifying the set of fuzzy parameters; formation of standards fuzzy parameters; forming sets of heuristic rules for detection and identification of incidents; phasing parameters monitored to identify incident; processing parameters and formation result. The proposed method can be used single or in combination with the method of assessing the criticality level of the situation due to the influence of the incident/potential crisis.

Index terms: crisis, incident, criticality level of crisis, expert methods, fuzzy set theory, detection and identification of crisis, integrated model.

Карпінський Микола Петрович, доктор техічних наук, професор, Голова Департаменту комп'ютерних наук та інженерії, Університет Бельсько-Бяла, Техніко-гуманітарна академія (м. Бельсько-Бяла, Польща).
E-mail: mpkarpinski@gmail.com.
Карпинский Николай Петрович, доктор технических наук, профессор, Глава департамента компютерных наук и инженерии, Университет Бельско-Бяла, Технико-гуманитарная академия.
Karpiński Mikołaj, D.Sn., Professor, Chairman of Department of Computer Science and Engineering University of Bielsko-Biala, Akademia Techniczno-Humanistyczna (Bielsko-Biala, Poland).

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 информа-

ционных технологий Национального авиационного университета.
Korchenko Anna, PhD in Eng., Associate Professor of Academic Department of IT.

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 Andrii, Assistant of Academic Department of IT-security, National Aviation University.

УДК 004.056

СКОРОСТНОЕ УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ НА ОСНОВЕ МНОГО ПОТОКОВЫХ ВЫЧИСЛЕНИЙ

Евгений Котух, ВладимирКарташов, Денис Цапко, Олег Халимов, Алина Самойлова

Универсальное хеширование определяет доказуемо стойкую аутентификацию со счетчиком, обеспечивает высокую стойкость к коллизиям и скорость вычислений. Одним из наиболее перспективных направлений в решении задач высокоскоростных вычислений является использование технологии GPGPU (General-purpose graphics processing units). Технология GPGPU позволяет на одном вычислителе достигать высокого уровня параллелизма без временных затрат на передачу данных между узлами и синхронизацию результатов вычислений. Для повышения скорости универсального хеширования на основе скалярных и полиномиальных вычислений разработаны предложения по много потоковым вычислениям, вычислениям в модулярной арифметике и арифметике над расширенным конечным полем с использованием GPGPU технологии.

***Ключевые слова**: универсальное хеширование, много потоковые вычисления, архитектура массивно-параллельных вычислений CUDA.*

ВВЕДЕНИЕ. В качестве основных составляющих прироста мощности вычислительных систем можно выделить: рост производительности выделенных вычислительных устройств; организацию массовых вычислений в совокупности устройств, в том числе и мобильных; использование эффективных моделей вычислений на существующих классах архитектур. Одним из наиболее перспективных направлений в решении задач вычислений общего назначения является использование технологии GPGPU (General-purpose graphics processing units) [1, 2]. Графический процессор (GPU) обладает меньшим набором исполняемых команд (RISC-подобные архитектуры), чем CPU, но большей производительностью. Технология GPGPU позволяет на одном вычислителе достигать достаточно высокого уровня параллелизма без временных затрат на передачу данных между узлами и синхронизацию результатов вычислений. Относительная низкая стоимость, простота добавления вычислительных модулей и удельное энергопотребление в сочетании с высокой удельной производительностью GPU позволяют реализовать на практике массовые распределенные параллельные вычисления, которые доступны более широкому кругу потенциальных нарушителей. Использование вычислений на GPGPU в решение целого ряда вычислительно сложных задач в области проблем криптографии представляет практический и научный интерес.

Широкое распространение получили алгоритмы шифрования и цифровой подписи (Эль-Гамаль, DSA, ГОСТ), стойкость которых основана на сложности решения задачи дискретного логарифмирования в мультипликативной группе числового поля и в группе точек эллиптической кривой над конечным полем. Особенностью данной задачи является быстрый рост времени выполнения при увеличении размера задачи. Эффективный алгоритм параллельного выполнения на GPGPU архитектуре, предназначенный для ускорения решения задачи дискетного логарифмирования в различных группах с помощью распределённых многопроцессорных вычислений представлены в работе [1]. Для вычисления дискретного логарифма в группе точек эллиптической кривой наиболее эффективным считается ρ-метод Полларда реализация которого на GPU в работе [3] дала 100-кратный прирост производительности по сравне-