© Gizun A., Lozova I., Trykush O. Appliance of incident/potential crisis situations correlation mechanism for assessment of current situation criticality level in information sphere // Ukrainian Scientific Journal of Information Security, 2017, vol. 23, issue 3, p.215-221.

DOI: 10.18372/2225-5036.23.12110

ЗАСТОСУВАННЯ МЕХАНІЗМУ КОРЕЛЯЦІЇ ІНЦИДЕНТІВ / ПОТЕНЦІЙНИХ КРИЗОВИХ СИТУАЦІЙ ДЛЯ ОЦІНЮВАННЯ РІВНЯ КРИТИЧНОСТІ ПОТОЧНОЇ СИТУАЦІЇ В ІНФОРМАЦІЙНІЙ СФЕРІ

Андрій Гізун, Ірина Лозова, Ольга Трикуш

Національний авіаційний університет, Україна

ГІЗУН Андрій Іванович, к.т.н.

Рік та місце народження: 1987 рік, м. Нетішин, Хмельницька область, Україна.
Освіта: Національний авіаційний університет, 2010 рік.
Посада: доцент кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, управління інцидентами інформаційної безпеки, комплексні системи захисту інформації, штучні імунні системи, управління безперервністю бізнесу та правове забезпечення захисту інформації.
Публікації: більше 50 наукових публікацій, серед яких наукові статті, матеріали і тези доповідей на конференціях, авторські свідоцтва.
E-mail: andriy.gizun@gmail.com

ЛОЗОВА Ірина Леонідівна

Рік та місце народження: 1983 рік, м. Енгельс, РФ.
Освіта: Національний авіаційний університет, 2005 рік.
Посада: старший викладач кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, криміналістичний аналіз комп'ютерних систем, криптографічний захист інформації, бази даних, управління безперервністю бізнесу.
Публікації: наукові статті, матеріали і тези доповідей на конференціях, авторські свідоцтва.
E-mail: illozovaya@gmail.com

ТРИКУШ Ольга Анатоліївна

Рік та місце народження: 1995 рік, м. Луцьк, Волинська область, Україна.
Освіта: Національний авіаційний університет, з 2012 року.
Посада: студентка 6 курсу кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, управління безперервністю бізнесу, управління кризовими ситуаціями.
Публікації: матеріали і тези доповідей на конференціях.
E-mail: trykush.olg@gmail.com.

Анотація. *Розвиток інформаційних технологій, комунікаційних систем та систем обробки інформації забезпечує оптимізацію процесів менеджменту підприємствами, установами та організаціями. Однак, разом із цим зростає залежність ефективного функціонування організації від рівня надання інформаційних послуг. Виникнення різного роду інцидентів інформаційної безпеки можуть серйозно вплинути на бізнес-процеси будь-якого підприємства, а при досягненні рівня їх впливу на інформаційну систему певного критичного значення виникає можливість появи кризової ситуації. На сьогодні запропоновані методи виявлення інцидентів / потенційних кризових ситуацій та оцінювання їх рівня критичності. Проте в даних методах не описані процедури узгодження появи декількох кризових ситуацій одночасно і визначення середнього та сумарного рівня критичності. В даній роботі розглянуті питання кореляції декількох подій – кризових ситуацій – і запропонований механізм обчислення середнього та сумарного рівня критичності інцидентів. В основі механізму кореляції подій, як власне і самих методів управління кризовими ситуаціями, лежать методи експертного оцінювання та моделі нечіткої логіки. Застосування запропонованого механізму дасть змогу врахувати одночасну появу декількох інцидентів і оцінити середній та сумарний вплив, який вони спричиняють на інформаційну систему.*

Ключові слова: *кризова ситуація, метод, система, менеджмент інформаційної безпеки, кореляція, концепція управління безперервністю бізнесу, механізм, рівень критичності, вплив, нечітка логіка, модель представлення кризових ситуації.*

Вступ

Стрімкий розвиток інформаційних технологій (ІТ) разом з зростанням можливостей комунікації та обробки інформаційних потоків породжує значне зростання кількості інцидентів/потенційних кризових ситуацій, що відображено в міжнародних статистичних звітах та матеріалах [1,2]. Враховуючи залежність процесів менеджменту організацій від інформаційних систем, концепція управління безперервністю бізнесу виходить на передові ролі в системі функціонування бізнесу та держави, причому взаємозв'язок ІТ та бізнес-процесів (БП) стає настільки тісним, що життєздатність підприємств повністю залежить від надійності технологій, що забезпечують підтримку найбільш важливих критичних БП підприємства, організації, установи.

Проблема реагування на кризові ситуації (КС) в сфері ІТ є надзвичайно важливою, хоча ще не достатньо вивченою. Сьогодні невпинно зростає роль систем реагування на кризові явища в процесі управління та підтримання життєздатності підприємств, установ та організацій усіх форм власності. У розвинених країнах ринок технологій і послуг, що забезпечують безперервність бізнесу (ББ), динамічно розвивається [3]. При цьому все більш актуальним стає забезпечення захисту від не катастрофічних, а, більш ймовірних надзвичайних ситуацій.

В роботах [4,5] описані методи виявлення та ідентифікації інцидентів / потенційних кризових ситуацій (ІПКС), а також оцінювання рівня критичності інцидентів, які засновані на нечіткій логіці та методах експертного оцінювання. В [6] описана інтегрована модель представлення ІПКС. На основі цих методів розроблений обчислювальний комплекс [7], що реалізує процеси управління ІПКС.

Проте в цих роботах неврахована ситуація появи декількох (двох і більше) ІПКС одночасно, їх узгодження та визначення середнього та сумарного рівня критичності. Тому основною метою даної статті є розробка механізму кореляції інцидентів інформаційної безпеки та визначення середнього та сумарного рівня критичності спричиненого ними впливу на інформаційну систему з застосуванням методів нечіткої логіки.

Основна частина дослідження

Для формалізації процесів прогнозування, виявлення, ідентифікації та оцінки КС введемо множину ІПКС:

$$\mathbf{IKS} = \{\bigcup_{i=1}^{n} \mathbf{IKS_i}\} = \{\mathbf{IKS_1}, \ldots, \mathbf{IKS_n}\},\ (i = \overline{1,n}), \qquad (1)$$

де n визначає кількість потенційних КС i, тобто інцидентів, що можуть спричинити кризовий стан, кожен з яких відображається у вигляді узагальненого шести компонентного кортежу [6]:

$$\mathbf{IKS_i} = < IKS_i,\ \mathbf{P_i},\ \mathbf{T_i^e},\ \underset{\sim}{\mathbf{P}}_{\mathbf{i}},\ \mathbf{ER_i},\ LCS_i >, \qquad (2)$$

в якому: IKS_i – ідентифікатор i-го ІПКС, що є (або може стати) причиною виникнення КС; $\mathbf{P_i}$ – підмножина можливих параметрів, що використовуються для прогнозування чи ідентифікації i-го інциденту; $\mathbf{T_i^e}$ – підмножина всіх можливих нечітких (лінгвістичних) еталонів, що відображають еталоні стани відповідних параметрів з підмножини $\mathbf{P_i}$; $\underset{\sim}{\mathbf{P}}_{\mathbf{i}}$ – підмножина поточних значень параметрів за певний проміжок часу; $\mathbf{ER_i}$ – підмножина евристичних правил, побудованих на основі нечітких параметрів, які використовуються для виявлення/ідентифікації i-го ІПКС; LCS_i – рівень критичності ситуації, спричиненої i-м ІПКС.

Детальний опис процедури виявлення, ідентифікації ІПКС, описаний в [5].

Виявлена ситуація відноситься до кризової лише якщо рівень її критичності вищий середнього або більший, тобто $LCS_i \gtrsim BC^e$. В іншому разі інцидент або взагалі залишається поза увагою (при достатньо низькому рівні критичності) або проводиться реагування на нього з метою контролю і усунення як для звичайного інциденту інформаційної безпеки.

Кожен інцидент характеризується рівнем критичності, що задається множиною $\mathbf{LCS} = \{\bigcup_{i=1}^{n} \underset{\sim}{LCS}_i\} = \{\underset{\sim}{LCS}_1, \ldots, \underset{\sim}{LCS}_n\},\ (i = \overline{1,n})$. Рівень критичності визначається через параметри оцінки критичності ситуації з врахуванням їх вагових коефіцієнтів, тобто $\underset{\sim}{LCS}_i = \sum_{e=1}^{E} (\Omega_e * \underset{\sim}{\mathrm{L}}_e)$. Встановлено, що рівень критичності можна описати врахувавши функціональні залежності між $\underset{\sim}{\mathrm{L}}_e$ – параметрами оцінки рівня критичності. Детально метод оцінювання рівня критичності та множина оціночних параметрів описані в роботі [4].

Недоліком даної моделі є неврахування взаємного впливу інцидентів, дія яких збігається у часі, на середовище інформаційної системи. Оскільки той чи інший ІПКС характеризується набором оціночних параметрів рівня критичності, що визначають ступінь впливу інциденту на середовище в певному аспекті, то кожен з ІПКС може посилювати загальний рівень впливу на систему залежно від величини їх кореляції один з одним. Так, коефіцієнт кореляції встановлює залежність між різними ІПКС і може набувати значень від 0 до 1. Причому ІПКС, які однорідно впливають на контрольоване середовище мають коефіцієнт кореляції рівний 1, а ІПКС, що спричиняють вплив в різних аспектах на відповідне середовище і їх взаємозалежність ніяк не проявляється під час визначення загального рівня критичності, мають значення коефіцієнта кореляції 0. Таким чином ІПКС, що корелюються між собою, підсилюють ефект впливу на середовище один одного, що можна відобразити у вигляді середнього та сумарного рівня критичності з врахуванням їх взаємозалежності, а не корельовані ІПКС спричинюють вплив, рівень якого можна оцінити лише для кожного інциденту окремо.

Виходячи з цих позицій запропонуємо застосування в моделі представлення ІПКС та методі оцінки рівня критичності поточної ситуації механізму кореляції подій. Даний механізм ґрунтується на визначенні спільних оціночних параметрів рівня

критичності для різних ІПКС, причому чим більша кількість однакових параметрів тим більший коефіцієнт кореляції.

Так кожен інцидент можна оцінити застосувавши загальний набір параметрів оцінки рівня критичності [4], такі як: «Тривалість інциденту (TR)», «Степінь порушення функціоналу критичних ресурсів/процесів (DVF)», «Географічний масштаб інциденту (GS)», «Масштаб інциденту в організаційному аспекті (OS)», «Загальний рівень економічних збитків (OLED)», «Відношення рівня економічних збитків за поточний період до відповідного рівня за попередній період (RD)», «Рівень загрози життю та здоров'ю людей (RTLH)», «Питомий показник смертності на поточний момент (RM)», «Частота проявів інцидентів (інтенсивність) (F)», «Степінь руйнування інфраструктури (DDI)», «Співвідношення орієнтовного часу відновлення і показника RTO (CRT)», «Відношення рівня втрат ресурсів і показника RPO (CRP)», «Рівень панічних, протестних та антидержавних настроїв персоналу/населення (LM)», «Степінь впливу зовнішніх дестабілізуючих та психологічних чинників (DIEPF)», «Степінь порушення характеристик безпеки ІР з ОД (DVChS)». Кількість і склад характерних параметрів для кожного ІПКС можуть мати різні значення і визначаються експертами.

Сам механізм має кілька етапів, зокрема:

1. Визначення кількості ІПКС, з якими проводяться операції, та наборів оціночних параметрів для кожного з них.

2. Визначення основного і залежних ІПКС. При цьому порядок запису множини ІПКС міняється таким чином, щоб основний інцидент мав 1-ий номер.

3. Визначення коефіцієнтів кореляції для кожного залежного та основного ІПКС відповідно.

Розглянемо кожен з цих етапів.

Основним елементом інтегрованої моделі представлення ІПКС є ідентифікатор IKS_i що зв'язує елемент множини $\mathbf{IKS}$ з певним інцидентом, який визначається через відповідне йому ім'я. Наприклад, при $n=5$ отримаємо: $\mathbf{IKS} = \{\bigcup_{i=1}^{5} \mathbf{IKS_i}\} = \{\mathbf{IKS_1}, \mathbf{IKS_2}, \mathbf{IKS_3}, \mathbf{IKS_4}, \mathbf{IKS_5}\} = \{\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}, \mathbf{E}\}$, де $\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}, \mathbf{E}$ – назви інцидентів. Відповідно для кожного з цих інцидентів характерні свої набори оціночних параметрів:

$$\mathbf{L_i} = \bigcup_{i=1}^{N} \left\{ \bigcup_{e=1}^{E} \underset{\sim}{L}_e \right\} = \bigcup_{i=1}^{N} \{\underset{\sim}{L}_1, \underset{\sim}{L}_2, ..., \underset{\sim}{L}_E\}, \; e = \overline{1, E}, \qquad (3)$$

де E – кількість параметрів. Наприклад, за умов дослідження для інциденту $\mathbf{A}$ при E=15, $\mathbf{L_A} = \left\{ \bigcup_{e=1}^{15} \underset{\sim}{L}_e \right\} = \{\underset{\sim}{L}_1, \underset{\sim}{L}_2, ..., \underset{\sim}{L}_{15}\} = \{TR, \; DVF, \; GS, \; OS, \; OLED, \; RD, \; RTLH, \; RM, \; F, \; DDI, \; CRT, \; CRP, \; LM, \; DIEPF, \; DVChS\}$.

Для визначення залежності між ІПКС введемо дві категорії подій: основна та залежні від неї інциденти. Можна виділити два способи розподілення і привласнення значення основної та залежних подій, такі як: за часом – ІПКС, який був виявлений першим набуває статусу основного, а всі інші – залежних від нього ІПКС; за рівнем критичності – статус основного ІПКС привласнюється інциденту з найбільшим рівнем критичності.

В такому разі необхідно провести процедуру ранжування ІПКС за рівнем критичності. Оцінки рівня критичності отримані під час роботи обчислювального комплексу [7]: зібрані відомості про КС формують значення оціночних параметрів, які обробляються (шляхом визначення коефіцієнту важливості, проведення їхньої фазифікації, обраховування як суми з врахуванням коефіцієнта важливості і дефазифікації) ПЗ СОКСv1.0 і визначають загальний рівень критичності ситуації, що склалася в результаті впливу ІПКС.

Вибір способу здійснюється експертом, тобто ґрунтується на суб'єктивній думці оператора системи чи експерта. Звісно, 2-ий спосіб є більш пріоритетним, оскільки в такому разі відсутня небезпека неврахування критично важливих аспектів впливу ІПКС на контрольоване середовище.

Оскільки коефіцієнт кореляції дає змогу оцінити залежність ІПКС між собою і направлений на оцінку середнього та сумарного впливу їх сукупності за певним аспектом, то можливий випадок коли основний ІПКС вибирається експертом або оператором системи, користувачем, виходячи з позицій який з аспектів КС він вважає найбільш загрозливим. Наприклад, якщо в пріоритеті людські життя, то відповідно основним буде обрано ІПКС, що несе найбільшу загрозу в цьому аспекті, або при умові критичності функціонування інформаційних систем – ІПКС, що переривають ці процеси або знижують якість їх надання.

Коефіцієнт кореляції показує однакові аспекти впливу різних ІПКС і визначається кількістю спільних параметрів між основною та залежною подіями. Запропонований механізм ґрунтується на послідовному визначені коефіцієнта кореляції основної і кожного залежного ІПКС за формулою:

$$K_{IKS_{осн} IKS_{зал_i}} = \frac{|(\mathbf{L_{осн}} \cap \mathbf{L_{зал_i}})|}{|\mathbf{L_{зал_i}}|}, \qquad (4)$$

до тих пір, поки не будуть враховані всі залежності між ІПКС, причому $\mathbf{L_{осн}}$ - множина оціночних параметрів основного ІПКС і $\mathbf{L_{зал}}$ - множина оціночних параметрів залежних ІПКС. Таким чином, як зазначалось раніше, коефіцієнт кореляції може приймати значення від 0 (абсолютно незалежні події) до 1 (повністю залежні події).

Далі розглянемо проблему визначення середнього та сумарного рівнів критичності для набору тих чи інших виявлених ІПКС. Зазначимо, що кожна з цих процедур може здійснюватися як з врахуванням кореляційної залежності між інцидентами, так і без нього.

Так, середній рівень критичності може характеризувати ситуацію, що склалася з погляду її розвитку в часовій перспективі, зокрема для формування прогнозів подальшого розвитку. Скористаємось для визначення середнього рівня критичності ситуації, що виникла впливом декількох одночасних інцидентів, наступними формулами:

– без врахування коефіцієнта кореляції:

$$\underset{\sim}{LCS}_{сер} = \frac{1}{N}\sum_{i=1}^{N}\underset{\sim}{LCS}_i , \qquad (5)$$

де $\underset{\sim}{LCS}_{сер}$ - середній рівень критичності декількох ІПКС з врахуванням залежності між ними, $\underset{\sim}{LCS}_{осн}$ - рівень критичності основного ІПКС, $\underset{\sim}{LCS}_i$ - рівень критичності *i*-ого ІПКС, N - загальна кількість інцидентів;

– з врахуванням коефіцієнта кореляції, що дасть змогу оцінити рівень критичності в конкретному аспекті прояву ідентифікованих ІПКС:

$$\underset{\sim}{LCS}^{K}_{сер} = \frac{1}{N}(\underset{\sim}{LCS}_{осн} + \sum_{i=2}^{N} K_{IKS_{осн}IKS_{заг_i}} * \underset{\sim}{LCS}_i) , \qquad (6)$$

де $\underset{\sim}{LCS}_{сер}$ - середній рівень критичності декількох ІПКС з врахуванням залежності між ними, $\underset{\sim}{LCS}_{осн}$ - рівень критичності основного ІПКС, $\underset{\sim}{LCS}_i$ - рівень критичності інших (залежних) ІПКС і $K_{IKS_{осн}IKS_{заг_i}}$ - коефіцієнт кореляції між основним та відповідним залежним ІПКС, N - загальна кількість інцидентів.

Схематично процес знаходження середнього рівня критичності ІПКС та відповідних коефіцієнтів кореляції зображено на Рис. 1.

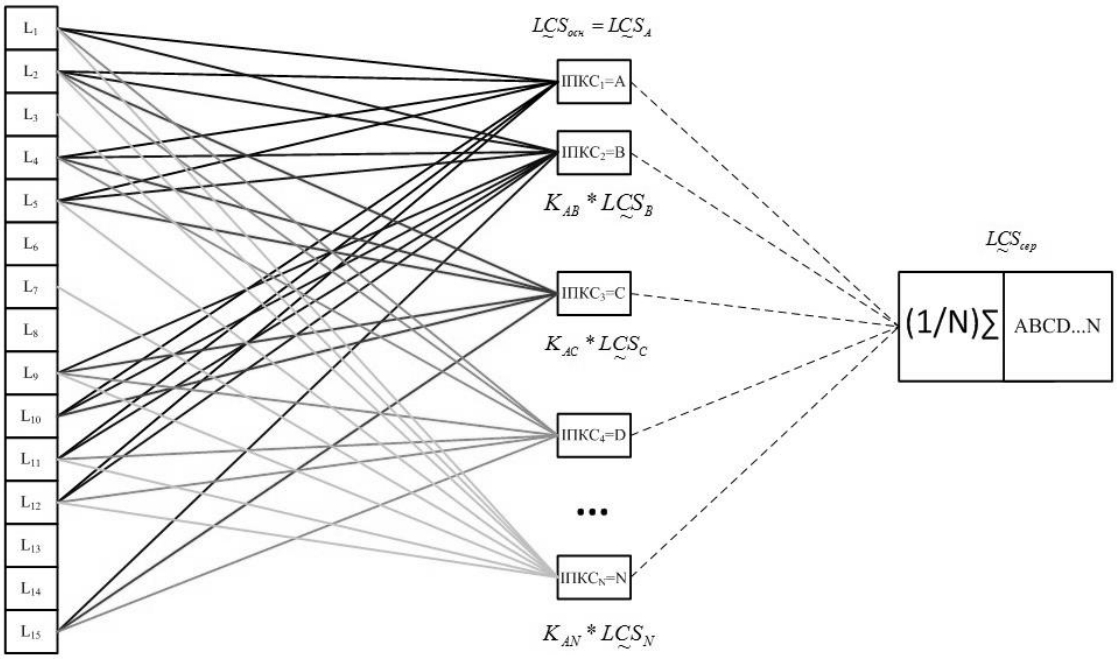

Рис. 1. Застосування механізму кореляції ІПКС для визначення середнього рівня критичності поточної ситуації, що склалася в умовах їх одночасного впливу

Сумарний рівень критичності ситуації, що виникла внаслідок впливу сукупності інцидентів важлива для вибору адекватних заходів для реагування на них. Це пояснюється тим, що контрзаходи, підібрані лише для одного ІПКС будуть не достатніми для нейтралізації їх сукупності, оскільки кожен інцидент привносить свою частку до зростаючого загального рівня.

У випадку, якщо рівень критичності окремого інциденту оцінюється від 0 до 100 балів, то ймовірно, що сумарний рівень буде перевищувати 100 балів. Така ситуація є недопустимою. Очевидно, що в такому разі визначення сумарного рівня не можна здійснювати банальним додаванням рівнів критичності окремих ІПКС.

Скористаємось для цього формулою Шортліффа, яка використовуються для визначення міри довіри двом і більше свідченням, що взаємопов'язані, в прийняті рішень експертними системами. Замінивши в ній «міру довіри» на «рівень критичності» зможемо її використати для нашої задачі.

Виведемо формулу для n-значення рівня критичності ІПКС. Так, для 2-ох ІПКС матимемо $\underset{\sim}{LCS}_{12} = \underset{\sim}{LCS}_1 + \underset{\sim}{LCS}_2(1 - \underset{\sim}{LCS}_1)$ або оскільки формула симетрична $\underset{\sim}{LCS}_{12} = \underset{\sim}{LCS}_2 + \underset{\sim}{LCS}_1(1 - \underset{\sim}{LCS}_2)$. Для 3-ох ІПКС - $\underset{\sim}{LCS}_{123} = \underset{\sim}{LCS}_3 + \underset{\sim}{LCS}_{12}(1 - \underset{\sim}{LCS}_3)$, а для 4-ох $\underset{\sim}{LCS}_{1234} = \underset{\sim}{LCS}_4 + \underset{\sim}{LCS}_{123}(1 - \underset{\sim}{LCS}_4)$. Підставивши у останній вираз аналітичні записи знаходження $\underset{\sim}{LCS}_{123}$ і $\underset{\sim}{LCS}_{12}$, провівши алгебраїчні перетворення отримаємо вираз для обчислення сумарного рівня критичності 4-ох ІПКС:

$$\underset{\sim}{LCS}_{1234} = \underset{\sim}{LCS}_4 + \underset{\sim}{LCS}_3(1 - \underset{\sim}{LCS}_4) + \underset{\sim}{LCS}_2(1 - \underset{\sim}{LCS}_3)$$
$$(1 - \underset{\sim}{LCS}_4) + \underset{\sim}{LCS}_1(1 - \underset{\sim}{LCS}_2)(1 - \underset{\sim}{LCS}_3)(1 - LCS_4) .$$

Узагальнивши і систематизувавши сформуємо формулу визначення сумарного рівня критичності для n інцидентів (потенційних кризових ситуацій) при відсутності кореляції між ними:

$$\underset{\sim}{LCS}_{сум} = \underset{\sim}{LCS}_N + \sum_{i=1}^{N-1}\underset{\sim}{LCS}_i \prod_{i=i+1}^{N}(1 - \underset{\sim}{LCS}_i) , \qquad (7)$$

де $\underset{\sim}{LCS}_{сум}$ - сумарний рівень критичності декількох ІПКС без врахуванням залежності між ними (кореляції), $\underset{\sim}{LCS}_i$ - рівень критичності *i*-ого ІПКС, N - загальна кількість інцидентів.

Аналогічно до середнього значення рівня критичності можемо застосувати до виявлених ІПКС механізм кореляції подій. Тоді сумарний рівень критичності з врахуванням залежності між окремими інци-

дентами в аспекті спричиненого ними впливу обчислимо за формулою:

$$\underset{\sim}{LCS}^{K}_{сум} = \underset{\sim}{LCS}^{K}_{N} + \sum_{i=1}^{N-1} \underset{\sim}{LCS}^{K}_{i} \prod_{i=i+1}^{N} (1 - \underset{\sim}{LCS}^{K}_{i}), \quad (8)$$

де $\underset{\sim}{LCS}^{K}_{сум}$ - сумарний рівень критичності декількох ІПКС з врахуванням кореляції між ними, N - загальна кількість інцидентів, $\underset{\sim}{LCS}^{K}_{i} = K_{IKS_{осн} IKS_{зал_i}} * \underset{\sim}{LCS}_{i}, i = \overline{2,N}$ - рівень критичності корельованого i-ого ІПКС, $\underset{\sim}{LCS}^{K}_{1} = \underset{\sim}{LCS}_{осн}$, N - загальна кількість інцидентів.

Експериментальне дослідження механізму кореляції та визначення середнього та сумарного рівнів критичності

Розглянемо роботу механізмів кореляції подій та оцінювання сумарного та середнього рівнів критичності ситуації, що склалась під впливом декількох ІПКС на прикладі.

Нехай A, B, C, D та E – ідентифікатори інцидентів, де A – Зміна кліматичних умов в серверній, B – Мережева атака відмова в обслуговувані, C – Крадіжка обладнання та носіїв інформації, D – Зламування мережі порушником, E – Повінь. Спочатку необхідно визначити множини оціночних параметрів, які відповідають кожному з них, для того, щоб виявити залежність між цими ІПКС.

Так, зміна кліматичних умов в серверній, характеризується такою множиною оціночних параметрів: $\mathbf{L_A} = \{ TR - L_1; DVF - L_2; OS - L_4; OLED - L_5; DDI - L_{10}; CRT - L_{11}; CRP - L_{12} \}$. Аналогічно для мережевої атаки відмова в обслуговувані: $\mathbf{L_B} = \{ TR - L_1; DVF - L_2; OS - L_4; OLED - L_5; F - L_9; DDI - L_{10}; CRT - L_{11}; CRP - L_{12}; DVChS - L_{15} \}$. Для крадіжка обладнання і носіїв інформації: $\mathbf{L_C} = \{ DVF - L_2; OS - L_4; OLED - L_5; F - L_9; DDI - L_{10}; DVChS - L_{15} \}$. Зламування мережі порушником характеризується множиною $\mathbf{L_D} = \{TR - L_1; DVF - L_2; OS - L_4; F - L_9; CRT - L_{11}; CRP - L_{12}; DVChS - L_{15} \}$. І останній ІПКС - повінь: $\mathbf{L_E} = \{TR - L_1; DVF - L_2; GS - L_3; OLED - L_5; RTLH - L_7; F - L_9; DDI - L_{10}; RTLH - L_7; CRP - L_{12} \}$.

Під час експериментального дослідження були промодельовані ІПКС і проведена їх оцінка за допомогою ПЗ СОКС [7] результати в чіткій і нечіткій формі, що наведені в табл. 1.

Результати оцінювання ІПКС Таблиця 1

ІПКС	Рівень критичності	НЧ
A	60 балів або 0,6	0/0,4; 1/0,6; 0/0,8
B	80 балів або 0,8	0/0,6; 1/0,8; 0/1
C	30 балів або 0,3	0/0,1;1/0,3;0/0,5
D	40 балів або 0,4	0/0,2; 1/0,4; 0/0,6
E	50 балів або 0,5	0/0,3; 1/0,5; 0/0,7

Припустимо, що в якості основного ІПКС експертом була обрана крадіжка обладнання і носіїв інформації, оскільки основний акцент в діяльності організації робиться на забезпеченні конфіденційності інформації. Далі визначаємо коефіцієнт кореляції між подіями, причому C – основний ІПКС, A,B,D,E – залежні. Тоді:

$$\underset{\sim}{LCS}_{C} = \underset{\sim}{LCS}_{осн} = \underset{\sim}{LCS}_{1}, \underset{\sim}{LCS}_{A} = \underset{\sim}{LCS}_{зал_2} = \underset{\sim}{LCS}_{2},$$
$$\underset{\sim}{LCS}_{B} = \underset{\sim}{LCS}_{зал_3} = \underset{\sim}{LCS}_{3}, \underset{\sim}{LCS}_{D} = \underset{\sim}{LCS}_{зал_4} = \underset{\sim}{LCS}_{4},$$
$$\underset{\sim}{LCS}_{E} = \underset{\sim}{LCS}_{зал_5} = \underset{\sim}{LCS}_{5}.$$

Розрахуємо коефіцієнти кореляції для обраних залежних подій, використовуючи вираз (4):

$$K_{12} = K_{CA} = K_{IKS_{осн} IKS_{зал_2}} = \frac{|(\mathbf{L_{осн}} \bigcap \mathbf{L_{зал_2}})|}{|\mathbf{L_{зал_2}}|} = \frac{|(\mathbf{L_C} \bigcap \mathbf{L_D})|}{|\mathbf{L_D}|} = \frac{4}{7},$$

$$K_{13} = K_{CB} = K_{IKS_{осн} IKS_{зал_3}} = \frac{|(\mathbf{L_C} \bigcap \mathbf{L_B})|}{|\mathbf{L_B}|} = \frac{6}{9} = \frac{2}{3},$$

$$K_{14} = K_{CD} = K_{IKS_{осн} IKS_{зал_4}} = \frac{|(\mathbf{L_C} \bigcap \mathbf{L_A})|}{|\mathbf{L_A}|} = \frac{4}{7},$$

$$K_{15} = K_{CE} = K_{IKS_{осн} IKS_{зал_5}} = \frac{|(\mathbf{L_C} \bigcap \mathbf{L_E})|}{|\mathbf{L_E}|} = \frac{3}{8}.$$

Таким чином, розраховані всі коефіцієнти кореляції для даного набору з 5-ти ІПКС.

Розрахуємо середній рівень критичності без врахування взаємозалежностей між окремими ІПКС, скориставшись формулою (5).

$$\underset{\sim}{LCS}_{сер} = \frac{1}{5}(\underset{\sim}{LCS}_{1} + \underset{\sim}{LCS}_{2} + \underset{\sim}{LCS}_{3} + \underset{\sim}{LCS}_{4} + \underset{\sim}{LCS}_{5}) =$$

(1/5)({0/0,1; 1/0,3; 0/0,5} + {0/0,2; 1/0,6; 0/0,8} + {0/0,6; 1/0,8; 0/1} + {0/0,2; 1/0,4; 0/0,6} + {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/0,3; 0/0,7; 0/0,9; 0/0,5; 1/0,9; 0/1,1; 0/0,7; 0/1,1; 0/1,3}+{0/0,6; 1/0,8; 0/1} + {0/0,2; 1/0,4; 0/0,6} + {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/0,7; 1/0,9; 0/1,1}+{0/0,6; 1/0,8; 0/1} + {0/0,2; 1/0,4; 0/0,6} + {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/1,3; 0/1,5; 0/1,7; 0/1,5; 1/1,7; 0/1,9; 0/1,7; 0/1,9; 0/2,1}+{0/0,2; 1/0,4; 0/0,6} + {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/1,5; 1/1,7; 0/1,9}+{0/0,2; 1/0,4; 0/0,6} + {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/1,5; 1/1,7; 0/1,9}+{0/0,2; 1/0,4; 0/0,6} + {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/1,7; 0/1,9; 0/2,1; 0/1,9; 1/2,1; 0/2,3; 0/2,1; 0/2,3; 0/2,5}+ {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/1,9; 1/2,1; 0/2,3}+ {0/0,3; 1/0,5; 0/0,7}) = (1/5)({0/2,2; 0/2,4; 0/2,6; 0/2,4; 1/2,6; 0/2,8; 0/2,6; 0/2,8; 0/3}) = (1/5)({0/2,4; 1/2,6; 0/2,8}) = {0/0,48; 1/0,52; 0/0,56}* або після дефазифікації $\underset{\sim}{LCS}_{сер} = 0{,}52$ або *52* бали за *100*-бальною шкалою.

Для того, щоб визначити середнє значення рівня критичності щодо окремого аспекту, зазвичай по якійсь окремій найважливішій характеристиці потрібно застосувати механізм кореляції. Оскільки система [7] дає змогу представити результати як в нечіткій так і чіткій формі, надалі будемо проводити розрахунки для спрощення обчислень використовуючи апарат звичайної (чіткої) арифметики. Визначимо середній рівень критичності поточної ситуації за виразом (6):

$$\underset{\sim}{LCS}^{K}_{сер} = \frac{1}{5}(\underset{\sim}{LCS}_{1} + \sum_{i=2}^{5} K_{IKS_{осн} IKS_{зал_i}} * \underset{\sim}{LCS}_{i}) = \quad (1/5)*$$

*(0,3 + (4/7)*0,6) + (2/3)*0,8 + (4/7)*0,4 + (3/8)*0,5) = 0,32* або *32* бали за *100*-бальною шкалою.

Як бачимо, середнє значення рівня критичності з врахуванням кореляції між інцидентами менше ніж без врахування, що пояснюється виділенням конкретного аспекту щодо оцінки впливу, за умов експерименту – збереження конфіденційності інформаційних ресурсів. Таким чином, той вплив, що породжує порушення інших характеристик, в даних розрахунках

не враховано. Для перевірки адекватності запропонованого механізму перевіримо коректність результатів при подачі у вигляді вхідних даних рівнів критичності всіх виявлених інцидентів, що становлять 0 і 1 (табл. 2 та табл. 3).

Результати оцінювання ІПКС Таблиця 2

ІПКС	Рівень критичності	НЧ
A	0	0/0; 1/0; 0/0,2
B	0	0/0; 1/0; 0/0,2
C	0	0/0; 1/0; 0/0,2
D	0	0/0; 1/0; 0/0,2
E	0	0/0; 1/0; 0/0,2

Очевидно, що коли рівень критичності всіх ІПКС буде 0 балів, то: $\underset{\sim}{LCS}_{сер} = \underset{\sim}{LCS}^{K}_{сер} = 0$.

Результати оцінювання ІПКС Таблиця 3

ІПКС	Рівень критичності	НЧ
A	100 балів або 1	0/0,8; 1/1; 0/1
B	100 балів або 1	0/0,8; 1/1; 0/1
C	100 балів або 1	0/0,8; 1/1; 0/1
D	100 балів або 1	0/0,8; 1/1; 0/1
E	100 балів або 1	0/0,8; 1/1; 0/1

Розрахуємо середній рівень критичності ситуації без врахування показників кореляції інцидентів в випадку коли всі ІПКС мають максимальну критичність. Відповідно до (5):

$$\underset{\sim}{LCS}_{сер} = \frac{1}{5}(\underset{\sim}{LCS}_1 + \underset{\sim}{LCS}_2 + \underset{\sim}{LCS}_3 + \underset{\sim}{LCS}_4 + \underset{\sim}{LCS}_5) =$$

1/5(1+1+1+1+1) = 1 або *100* балів.

З врахування кореляційної взаємозалежності інцидентів згідно з формулою (6):

$$\underset{\sim}{LCS}^{K}_{сер} = \frac{1}{5}(\underset{\sim}{LCS}_1 + \sum_{i=2}^{5} K_{IKS_{осн} IKS_{заг_i}} * \underset{\sim}{LCS}_i) = (1/5)*$$

*(1 + (4/7)*1) + (2/3)*1 + (4/7)*1 + (3/8)*1) = 0,64* або *64* бали за *100*-бальною шкалою.

Як видно, отримані результати цілком коректні і не виходять за область допустимих значень рівня критичності $[0;1]$.

Проаналізуємо коректність застосування механізму визначення сумарного рівня критичності ситуації в залежності від врахування взаємної кореляції інцидентів.

Розрахуємо сумарний рівень критичності без врахування взаємозалежностей між окремими ІПКС, скориставшись формулою (7):

$$\underset{\sim}{LCS}_{сум} = \underset{\sim}{LCS}_5 + \sum_{i=1}^{4} \underset{\sim}{LCS}_i \prod_{i=i+1}^{5} (1 - \underset{\sim}{LCS}_i) =$$

0,5+0,3((1-0,6) (1-0,8)(1-0,4)(1-0,5)) + 0,6((1-0,8) (1-0,4) (1-0,5)) + 0,8((1-0,4)(1-0,5))+0,4(1-0,5)= 0,5+0,0072+0,036+0,24+0,2=0,9832 або *98* балів за *100*-бальною шкалою.

Застосуємо механізм кореляції інцидентів, щоб визначити сумарний рівень критичності ситуації, що склалася внаслідок їх комплексного впливу. Визначимо сумарний рівень критичності поточної ситуації за виразом (8), причому коефіцієнти кореляції застосуємо такі ж як в попередньому прикладі, тобто: $K_{12} = \frac{4}{7}$, $K_{13} = \frac{2}{3}$, $K_{14} = \frac{4}{7}$, $K_{15} = \frac{3}{8}$, а вхідні дані з табл. 1.

Відповідно $\underset{\sim}{LCS}^{K}_2 = K_{12} * \underset{\sim}{LCS}_2$, $\underset{\sim}{LCS}^{K}_3 = K_{13} * \underset{\sim}{LCS}_3$, $\underset{\sim}{LCS}^{K}_4 = K_{14} * \underset{\sim}{LCS}_4$, $\underset{\sim}{LCS}^{K}_5 = K_{15} * \underset{\sim}{LCS}_5$ і $\underset{\sim}{LCS}^{K}_1 = \underset{\sim}{LCS}_1$.

Отже, $\underset{\sim}{LCS}^{K}_{сум} = \underset{\sim}{LCS}^{K}_5 + \sum_{i=1}^{4} \underset{\sim}{LCS}^{K}_i \prod_{i=i+1}^{5} (1 - \underset{\sim}{LCS}^{K}_i) =$

(3/8)0,5 + 0,3((1-(4/7)0,6)(1-(2/3)0,8)(1-(4/7)0,4)(1-(3/8)0,5)) + (4/7)0,6 ((1-(2/3)0,8)(1-(4/7)0,4)(1-(3/8)0,5)) + (2/3)0,8((1-(4/7)0,4)(1-(3/8)0,5)) + (4/7)0,4(1-(3/8)0,5) = 0,1875 + 0,0577 + 0,1003 + 0,3343 + 0,1857 = 0,8655 або *87* балів за *100*-бальною шкалою.

Як бачимо, сумарне значення рівня критичності з врахуванням кореляції між інцидентами менше ніж без врахування, що також пояснюється виділенням конкретного аспекту щодо оцінки впливу, за умов експерименту – збереження конфіденційності інформаційних ресурсів. Таким чином, той вплив, що породжує порушення інших характеристик, в даних розрахунках не враховано.

Для перевірки адекватності запропонованого механізму перевіримо коректність результатів при подачі у вигляді вхідних даних рівнів критичності всіх виявлених інцидентів, що становлять 0 і 1 (табл. 2 та табл. 3 відповідно).

Очевидно, що коли рівень критичності всіх ІПКС буде 0 балів, то $\underset{\sim}{LCS}_{сум} = \underset{\sim}{LCS}^{K}_{сум} = 0$.

Розглянемо ситуацію, яка виникає під впливом інцидентів з максимальною критичністю. Розрахуємо сумарний рівень критичності ситуації без врахування показників кореляції інцидентів в такому випадку. Відповідно до (7):

$$\underset{\sim}{LCS}_{сум} = \underset{\sim}{LCS}_5 + \sum_{i=1}^{4} \underset{\sim}{LCS}_i \prod_{i=2}^{5} (1 - \underset{\sim}{LCS}_i) = 1 + 1 ((1-1)(1-1)(1-1)(1-1)) + 1((1-1)(1-1)(1-1)) + 0,8((1-1)(1-1)) + 1(1-1) = 1$$

або *100* балів.

З врахування кореляційної взаємозалежності інцидентів згідно з формулою (8):

$$\underset{\sim}{LCS}^{K}_{сум} = \underset{\sim}{LCS}^{K}_5 + \sum_{i=1}^{4} \underset{\sim}{LCS}^{K}_i \prod_{i=2}^{5} (1 - \underset{\sim}{LCS}^{K}_i) = (3/8) +$$

(1-(4/7))(1-(2/3))(1-(4/7))(1-(3/8)) + (4/7)(1-(2/3))(1-(4/7))(1-(3/8)) + (2/3)(1-(4/7))(1-(3/8)) + (4/7)(1-(3/8)) = 0,375 + 0,038265 + 0,05102 + 0,178571 + 0,357143 = 1 або *100* балів за *100*-бальною шкалою.

Як видно отримані результати, так само як і при визначені середнього рівня критичності, цілком коректні і не виходять за область допустимих значень $[0;1]$, що підтверджує адекватність розроблених механізмів.

Висновки

Запропонований механізм кореляції, основними етапами якого є: 1) вибір ІПКС та наборів оціночних параметрів з загальної множини, що характеризують їх вплив на середовище; 2) вибір основного і залежних ІПКС, а також відповідна зміна нумерації інцидентів в системі; 3) визначення коефіцієнта кореляції кожного залежного ІПКС з основним, що визначає взаємозалежності між ними. Отримані коефіцієнти кореляції можуть бути використані для обчислення середнього та сумарного рівнів критичності ситуації, що виникла під впливом декількох взаємопов'язаних і одночасних інцидентів (потенційних кризових ситуацій) В основі механізму, так як і в методах виявлення

та оцінювання ІПКС, лежать методи нечіткої логіки та експертного оцінювання. Коефіцієнти кореляції визначають спільні ознаки впливу кожного з інцидентів на систему чи середовище, що захищаються, і визначаються шляхом співставлення параметрів оцінки рівня критичності кожного ІПКС.

Практичне та наукове значення даного механізму полягає в можливості оцінювання одночасного впливу декількох ІПКС в певному аспекті на стан контрольованого середовища. Крім того, визначення середнього рівня критичності дасть змогу оцінити ситуацію, що склалася з статистичної точки зору і зробити прогнози подальшого її розвитку. Сумарний рівень критичності дозволяє здійснити адекватний рівню небезпеки вибір контрзаходів. А застосування кореляції інцидентів між собою дозволяють вирішувати такі задачі з отриманням оцінок в конкретному аспекті загроз інформаційній, національній чим іншій безпеці.

Література

[1] EM–DAT: The OFDA/CRED International Disaster Database, Brussels, Belgium, [Online]. Available at: http: //www.em–dat.net

[2] D. Guha–Sapir, F. Vos, R. Below, S. Ponserre, «Annual Disaster Statistical Review 2010», *Centre for Research on the Epidemiology of Disasters (CRED)*, [Online]. Available at:: http://www.cred.be/sites/default/files/ADSR_2010.pdf

[3] С. Петренко, А. Беляєв, «Управление непрерывностью бизнеса. Ваш бизнес будет продолжаться», М.: ДМК–Пресс, Компания АйТи, 400 с., 2011.

[4] А. Корченко, В. Козачок, А. Гізун, «Метод оцінки рівня критичності для систем управління кризовими ситуаціями», *Захист інформації*, Т.17, №1, с. 86-98, 2015.

[5] М. Карпінський, А. Корченко, А. Гізун, «Метод виявлення інцидентів/потенційних кризових ситуацій», *Захист інформації*, Т.17, №2, с.124-130, 2015.

[6] М. Карпінський, А. Корченко, А.Гізун, «Інтегрована модель представлення кризових ситуацій та формалізована процедура побудови еталонів ідентифікуючих параметрів», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, №.1 (29), с. 76-85, 2015.

[7] А. Гізун, «Обчислювальний комплекс виявлення та оцінювання кризових ситуацій в інформаційній сфері», *Захист інформації*, Т.18, №1, с. 66-73, 2016.

УДК 004.056.53:004.492.3 (045)

Гизун А.И., Лозова И.Л. Трикуш О.А. Применение механизма корреляции инцидентов / потенциальных кризисных ситуаций для оценки суммарного уровня критичности текущей ситуации в информационной сфере

Аннотация. *Развитие информационных технологий, коммуникационных систем и систем обработки информации обеспечивает оптимизацию процессов управления предприятиями, учреждениями и организациями. Однако вместе с этим растет зависимость эффективного функционирования организации от уровня оказания информационных услуг. Возникновения разного рода инцидентов информационной безопасности могут серьезно повлиять на бизнес-процессы любого предприятия, а при достижении уровня их влияния на информационную систему определенного критического значения возникает возможность появления кризисной ситуации. На сегодня предложены методы выявления инцидентов / потенциальных кризисных ситуаций и оценки их уровня критичности. Однако в данных методах не описаны процедуры согласования появления нескольких кризисных ситуаций одновременно и определения суммарного уровня критичности. В данной работе рассмотрены вопросы корреляции нескольких событий - кризисных ситуаций - и предложен механизм расчета суммарного уровня критичности инцидентов. В основе механизма корреляции событий, как собственно и самих методов управления кризисными ситуациями, лежат методы экспертного оценивания и модели нечеткой логики. Применение предложенного механизма позволит учесть одновременное появление нескольких инцидентов и оценить суммарный влияние, которое они оказывают на информационную систему.*

Ключевые слова: *кризисная ситуация, метод, система, менеджмент информационной безопасности, корреляция, концепция управления непрерывностью бизнеса, механизм, уровень критичности, влияние, нечеткая логика, модель представления кризисных ситуаций.*

Gizun A., Lozova I., Trykush O. Appliance of incident / potential crisis situations correlation mechanism for assessment of current situation criticality level in information sphere

Abstract. *The development of information technologies, communication systems and information processing systems provide optimization of management processes for enterprises, institutions and organizations. However, with this increased dependence of organization effective functioning from the level of providing information services. The emergence of various types of information security incidents can seriously affect the business processes of any enterprise, and when the level of their influence on the information system reach certain critical value, possibility of crisis situation occurrence arises. Methods of identifying incidents/potential crisis situations and assessing their criticality are already proposed. However, these methods do not describe the procedures for coordinating the emergence of several crisis situations at the same time and determination of the average and total level of criticality. In this work, the issues of several events (crisis situations) correlation are considered and proposed mechanism for calculating the average and total level of criticality for incidents. This events correlation mechanism is based on methods of expert evaluation and fuzzy logic models. The application of the proposed mechanism will make it possible to take into account the simultaneous occurrence of several incidents and assess the average and total impact that they have on information system.*

Key words: *crisis situation, method, system, information security management, correlation, business continuity management concept, mechanism, criticality level, influence, fuzzy logic, model of crisis situation presentation.*

Отримано *18 жовтня 2017 року*, затверджено редколегією *1 листопада 2017 року*