УДК 004.891.3:004.056

Іванченко Є.В., Гавриленко О.В., Гізун А.І.

БАЗОВА АРХІТЕКТУРА ЕКСПЕРТНОЇ СИСТЕМИ ПРОГНОЗУВАННЯ ТА ПОПЕРЕДЖЕННЯ КРИЗОВИХ СИТУАЦІЙ

У статті розглянуто проблеми захисту ресурсів інформаційних систем в умовах дії кризових ситуацій. Проаналізовані статистичні дані щодо кризових ситуацій різного (природного, техногенного, соціального) походження та дані стосовно існуючих розробок технічних систем управління процесами безперервності бізнесу. У роботі запропонована архітектура експертної системи прогнозування та попередження кризових ситуацій, що складається з двох підсистем: підсистеми прогнозування і ідентифікації кризових ситуацій та підсистеми нейтралізації впливу кризових ситуацій. Така система надає можливість забезпечувати управління безперервністю бізнесу на всіх стадіях, зазначених в стандартах та типових планах безперервності бізнесу: прогнозування, виявлення та ідентифікація кризових ситуацій, управління процесами нейтралізації і ліквідації наслідків кризових ситуацій.

Ключові слова: управління безперервністю бізнесу, кризова ситуація, експертна система, архітектура системи, прогнозування, інформаційні системи та ресурси, модуль, кортеж.

Вступ. Однією з найбільш суттєвих і розповсюджених загроз безпеці будь-якого підприємства, установи чи організації (інформаційній, фізичній, економічно-фінансовій, безпеці загалом) є кризові ситуації (КС). КС мають значний вплив на функціонування підприємств та організацій, оскільки будь-яка КС може вивести з ладу інформаційні, комунікаційні, технологічні підсистеми або навіть і зруйнувати саму будівлю установи.

Останні статистичні дані чітко показують ріст числа КС різного роду та характеру. Так наведені в [1] статистичні дані чітко показують, що кількість гідрометеорологічних кризових ситуацій на 2000 рік в порівнянні з 1950 зросла майже в 25 раз, геологічних – в 8 раз, а біологічних – близько в 50. За даними [2] у 2010 році кількість зареєстрованих лих наближається до середнього значення протягом 2000-2009 років (387). Число жертв зросло з 198 700 000 у 2009 році до 217,3 млн. в 2010 році, але залишилася нижче середньорічного числа жертв 227500000 протягом 2000-2009 років. Економічні збитки від стихійних лих в 2010 році більш ніж в 2,5 рази вищі ніж в 2009 (47,6 млрд. $ США) і збільшились на 25,3% в порівнянні з середньорічним показником (98,9 млрд. $ США).

Для вирішення проблеми управління бізнес-процесами і інформаційними ресурсами в умовах дії КС була створена концепція управління безперервністю бізнесу (УББ), що на даний момент є одним з найбільш актуальних напрямків стратегічного та оперативного менеджменту, що динамічно розвивається [3].

На сьогоднішній день процеси УББ описані в міжнародних стандартах та специфікаціях, серед яких слід відмітити BS ISO/IEC 17799:2005, BS 25999, NIST ST800-34, NFPA 1600, AS/NZ 5050, SS540:2008, COOP, HIPAA Gramm-Leach-Bliley, The Expedited Funds Availability, SAS 78/94. Процеси УББ висвітлюються в роботах таких авторів як С.А. Петренко, А.В. Бєляєв, Я. Ван Бон, С. Харріс та інших. Також підходи, що пов'язані з вирішення кризових ситуацій розглянуті в роботах К.В. Мусатова, А.В. Радіонова, С.А. Петренка, технології забезпечення неперервності ІТ-сервісів в надзвичайних ситуаціях досліджені в роботах Б.Д. Альтермана, Р.В. Лукичева, В.В. Задорожного.

Аналіз робіт [3-9] показав достатній розвиток нормативно-правової бази концепції УББ, її організаційних методів (створення аварійних груп реагування, процеси BIA - аналізу впливу на бізнес тощо). Проте з точки зору технічної реалізації на даний момент розроблені лише програмні засоби для розрахунку ризиків та для документаційного оформлення так званого плану забезпечення безперервності бізнесу (Business Continuity Plan - BCP). Існують поодинокі рішення в гірничодобувній галузі, розробки МНС Росії, але вони не охоплюють повний цикл УББ та не застосовуються для захисту ресурсів інформаційних систем. Жодне з запропонованих рішень не дає можливості забезпечення УББ на всіх стадіях, зазначених в стандартах та типових BCP: прогнозування, виявлення та ідентифікація КС, управління процесами нейтралізації і ліквідації наслідків КС. Значною проблемою є практична відсутність систем прогнозування КС та реагування на них, працюючих в автоматичному або принаймні напівавтоматичному режимі, яка б застосовувалася для вирішення широкого кола

проблем (насамперед стосовно захисту інформації) [10, 11]. Оскільки непередбачуваність власне КС змушує працювати персонал в умовах невизначеності, з вимогою підвищеної відповідальності та швидкості прийняття рішень. Зрозуміло, що автоматизація процесів прогнозування КС, прийняття рішення та підтримки процесів реалізації антикризових заходів була б дуже доцільною і є актуальною задачею.

Метою даної роботи є розробка архітектури ефективної експертної системи прогнозування та попередження кризових ситуацій (ЕСППКС) на підприємстві. Причому ефективність в даній роботі визначається такими параметрами: 1) охоплення всіх стадій УББ в умовах дії КС; 2) виявлення КС і невелика частота появи помилок 1-ого та 2-ого роду.

Основна частина. Передусім визначимо функції ЕСППКС. Відповідно до стандартів УББ [4-7] та типових планів ВСР розроблювана системи повинна виконувати наступні функції: збір та аналіз даних з навколишнього середовища, формування рішення (попередження) про можливість настання КС на основі порівняння зібраної інформації з даними бази даних системи, тобто її прогнозування, формування переліку необхідних заходів щодо нейтралізації впливу КС, а також, за можливістю, і автоматична підтримка їх виконання.

Виходячи з вищезазначених функцій розробимо архітектуру системи. ЕСППКС вміщує в собі дві підсистеми – підсистему прогнозування і ідентифікації КС (ППІКС) та підсистему нейтралізації впливу КС та зменшення рівня руйнувань, спричинених ними (ПНВКС). На рис. 1 зображена архітектура ППІКС, причому підсистема представлена в вигляді окремих модулів, а ПНВКС, що входить до складу ЕСППКС, – одним суцільним модулем. Вхідними даними ЕСППКС є параметри навколишнього середовища (атмосферний тиск, швидкість вітру, рівень опадів і т.п.) та підсистем підприємства (особливості передачі трафіку в інформаційно-комунікаційних системах, характеристики струму в електромережі, тиск рідини або газу в водо- та газокомунікаціях тощо) P_i, де і - ідентифікатор параметра (чинника), i=1..n. Вхідні дані, в залежності від їх природи, приймаються та фіксуються екологічними та технічними датчиками. Дані датчики входять до модулю фіксації вхідних даних (модуль первинних датчиків).

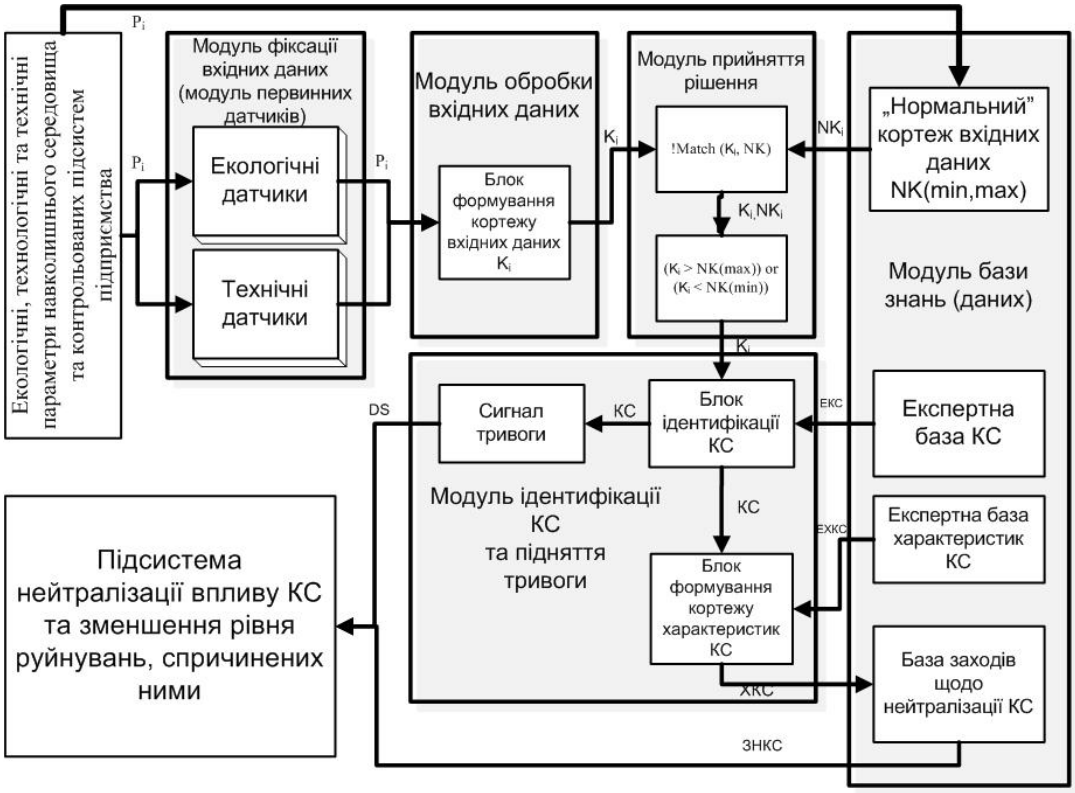

Рис. 1. Архітектура ЕСППКС

З вхідних даних, зібраних в тестовому режимі роботи системи, формуються так звані «нормальні» кортежі вхідних даних NK_i, що представляє собою набір значень

контрольованих параметрів або їх діапазонів в межах норми (відсутності КС). Можливе також формування, корекція та редагування "нормального" кортежу експертами. «Нормальний» кортеж вхідних даних зберігається в модулі бази знань разом з експертними базами КС і їх характеристик та базою заходів щодо нейтралізації КС, сформованими експертами – спеціалістами по КС.

Зафіксовані кожним датчиком в певний момент часу параметри P_i передаються до модуля обробки вхідних даних, де з них формуються кортежі вхідних даних в j-ий момент часу $K_{ij}=<K_{i0}, K_{i1},..,K_{im}>$, де j=1..m. Сформовані кортежі передаються в модуль прийняття рішення, в якому вони порівнюється з NK_i. У випадку якщо хоч один з елементів кортежу K_i відрізняється від відповідного елемента NK_i або не входить в дозволений діапазон приймається рішення про настання стану КС.

У модулі ідентифікації КС та підняті тривоги визначається власне тип КС та його характеристики з використанням інформації з експертної бази КС і експертної бази характеристик КС. Потім піднімається сигнал тривоги DS і паралельно відправляється запит до бази заходів щодо нейтралізації КС в модулі бази знань. Відповіддю на запит є виведення рекомендацій стосовно необхідних дій в стані КС – вхідних параметрів підсистеми нейтралізації впливу КС. Спрогнозувавши КС і виконавши запобіжні заходи не завжди можна досягнути ефекту повного захисту. ПНВКС по суті є другим захисним кордоном підприємства від впливу КС. Підсистема контролює та управляє зовнішніми обслуговуючими комунікаціями (водо- та газопроводами, лініями електропередач), щоб пом'якшити небезпеку під час лиха або інших надзвичайних ситуацій. Після виникнення КС система за потреби формує рішення про від'єднання зовнішніх комунікацій. При відсутності загрози комунікації знову від'єднуються. Функціонування ПНВКС подібне до роботи системи описаної в [12]. На рис. 2 зображена архітектура ПНВКС, причому підсистема представлена в вигляді окремих модулів, а ППІКС, що входить до складу ЕСППКС, – одним суцільним модулем. Робота ПНВКС запускається в момент отримання сигналу тривоги DS, який формується в модулі ідентифікації КС та підняті тривоги ППІКС і поступає разом з рекомендаціями стосовно необхідних дій в стані КС. Вхідними даними власне підсистеми в даному випадку виступають параметри середовища будівлі враженої КС (наявність вогню, підтоплення, концентрація газу в приміщені тощо) і параметри стану самих комунікацій (наявність розривів і т.п.). Вони приймаються спеціальними датчиками, на виході яких знаходиться не математична (числова) величина як в первинних датчиках, а лише наявність чи відсутність певного чинника: датчиками контролю приміщення - перші і датчиками контролю комунікацій - другі. Обидві групи датчиків входять до модулю вторинних датчиків.

Зібрані датчиками контролю приміщення дані передаються до модуля обробки. Тут вони формуються в один окремий кортеж $KP_p=<KP_0,KP_1,..,KP_l>$, p=1..*l* на основі якого приймається рішення про доцільність від'єднання чи збереження в робочому стані комунікацій.

Сформований кортеж передається до модуля прийняття рішень, куди також передаються дані з датчиків контролю комунікацій. Отримана послідовність P з кортежу KP_p і даних стану комунікацій $D_k=<D_0, D_1, ..., D_N>$, k=1..N, де N - кількість контрольованих комунікацій, порівнюється з послідовностями PN з бази знань ПНВКС.

База знань формується експертами і вміщує в собі можливі варіанти кортежів станів комунікацій і відповідні їм рішення. При співпадінні порівнюваних послідовностей приймається відповідне їм рішення U_k, k=1..N. Наприклад, при фіксації датчиками контролю приміщення пожежі і збережені цілісності водопроводів приймається рішення про припинення подачі газу, вимкнення ліній електропередач, проте зберігається подача води, що може бути корисним в процесі гасіння.

Прийняте рішення U_k передається до блоку управління кожної з комунікацій, яка і здійснює від'єднання приміщення від комунікацій, а також їх повторне підключення. Оскільки кількість і види контрольованих комунікацій за потреби можуть бути змінені відповідно змінюється і модуль управління комунікаціями. Підсистема працює циклічно з

певним періодом. При зникненні деяких з чинників КС чи появі нових ПНВКС знову приймає рішення про підключення/відключення комунікацій.

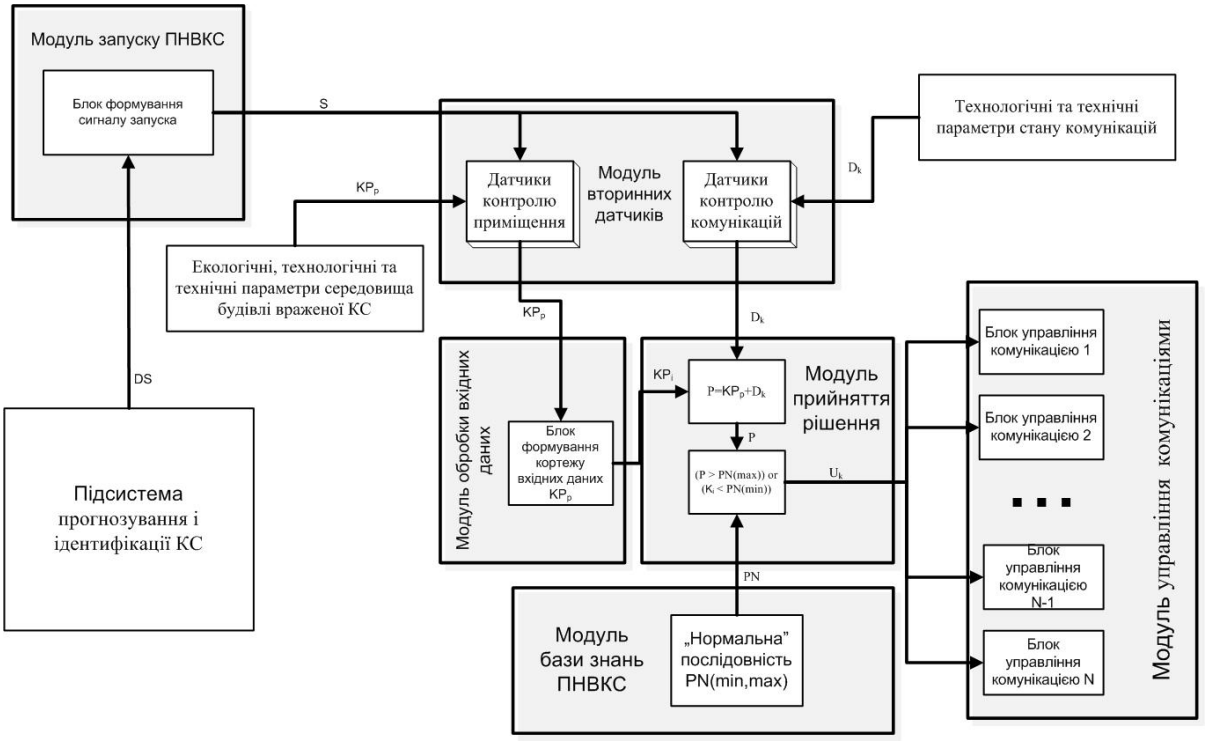

Рис. 2. Архітектура ПНВКС

Висновки. У основу запропонованої архітектури ЕСППКС входять дві підсистеми – ППІКС та ПНВКС. ППІКС, що складається з 5 модулів, а саме з модуля фіксації вхідних даних, обробки вхідних даних, прийняття рішення, ідентифікації КС та підняття тривоги і бази знань (даних), є першим захисним кордоном підприємства. ПНВКС, що складається з 6 модулів, а саме з модуля запуску ПНВКС, вторинних датчиків, обробки вхідних даних, прийняття рішення, управління комунікаціями і бази знань, є другим захисним кордоном підприємства.

Також в роботі представлені структурно-логічні зв'язки між модулями обох підсистем. Крім того в роботі наведені структурно-логічні зв'язки між власне двома підсистемами. Дана система є ефективною, оскільки надає можливість прогнозування та ідентифікації КС і забезпечувати підтримку процесів ліквідації їх наслідків, тобто охоплює всі стадії УББ.

У наступних роботах доцільно більш детально розглянути процедуру формування кортежів, пороговий механізм в модулях прийняття рішення ПНВКС та ППІКС, дослідити частоти появи помилок 1-ого та 2-ого роду.

ЛІТЕРАТУРА

1. EM-DAT: The OFDA/CRED International Disaster Database [Електронний ресурс] / UCL - Brussels, Belgium. – Режим доступу: http: //www.em-dat.net.

2. Guha-Sapir D. Annual Disaster Statistical Review 2010 [Електронний ресурс] / Debby Guha-Sapir, Femke Vos, Regina Below, Sylvain Ponserre // Centre for Research on the Epidemiology of Disasters (CRED). – Режим доступу: http://www.cred.be/sites/default/files/ADSR_2010.pdf.

3. Петренко С.А., Беляев А.В. Управление непрерывностью бизнеса. Ваш бизнес будет продолжаться / С.А. Петренко, А.В. Беляев. – М.: ДМК Пресс, Компания АйТи, 2011. – 400 с.

4. Business continuity management. Code of practice: BS25999-1:2006 – BSI British Standards, 2006 – 28p.

5. Business continuity management. Specification: BS25999-2:2007 – BSI British Standards, 2007. – 38p.

6. Singapore Standard for Business Continuity Management: SS540:2008 – SPRING Singapore, 2008. – 54p.

7. Business continuity – Managinig disruption-related risk: AS/NZS 5050 – Standards Australia, 2010. – 53p.

8. Van Bon Jan. ИТ СЕРВИС–МЕНЕДЖМЕНТ. Вводный курс на основе ITIL / Jan Van Bon. – Van Haren Publishing, по заказу ITSMF Netherlands, 2003. – 72 с.

9. Harris S. CISSP Certification All-in-One Exam Guide. – 5th edition. – Mc Graw-Hill Osborne Media,

2010. – 1216 p.

10. Морозов А.А. Ситуационные центры – основа стратегического управления / А.А. Морозов, В.А. Ященко // Математичні машини і системи. – 2003. – № 1. – С. 3 – 14.

11. Экспертные системы. Принципы работы и примеры / А. Брукинг, П. Джонс, Ф. Кокс и др.; под ред. Р. Форсайта – М.: Радио и связь, 1987. – 224с.

12. Patent No.: US 6266579 Bl. System for reducing disaster damage / Mohammad Reza Baraty. – № 09/022.667; заявл. February 12, 1998; опубл. July 24, 2001.

Надійшла: 07.07.2012 р.

Рецензент: д.т.н., професор Хорошко В.О.

УДК 004.056.53

Баранов Г.Л., Захарова М.В., Горніцька Д.А.

МЕТОДОЛОГІЯ СИНТЕЗУ СИСТЕМ ОЦІНКИ РІВНЯ ЗАХИЩЕНОСТІ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ ВІД СОЦІОТЕХНІЧНИХ АТАК

У роботі представлено методологію синтезу систем аналізу та оцінки рівня захищеності державних інформаційних ресурсів від соціотехнічних атак, які у наш час становлять одну з найбільших загроз і суттєво впливають на загальний рівень інформаційної безпеки. Розроблена методологія є гнучким інструментом та дає можливість здійснювати оцінювання рівня підготовленості персоналу до соціотехнічних атак на різних за специфікою роботи, управління, технічною базою підприємствах. Перевагами запропонованої методології є застосування такого параметру, як якість експерта, з метою підвищення якості експертного оцінювання загороз, та використання логіко-лінгвістичного підходу і математичного апарату нечіткої логіки, що дає можливість формалізувати оцінку ризиків.

Ключові слова: методологія синтезу систем аналізу та оцінки ризику, рівень захищеності, інформаційна безпека, соціотехнічні атаки, ризик, оцінка ризику.

Розвиток інформаційного суспільства розширив можливості інформаційного обміну, що в свою чергу дало поштовх удосконаленню існуючих та розвитку нових методів атак на державні інформаційні ресурси (ДІР), під якими слід розуміти взаємопов'язану, впорядковану, систематизовану, втілену на матеріальних носіях інформацію, створену або зібрану на законних підставах органами державної влади або іншими суб'єктами за рахунок державного бюджету [1].

В останні роки набули розвитку методи соціального інжинірингу, які відносяться до соціотехнічних атак (СА) [2-5]. Всі атаки даного класу засновані на переконані персоналу в санкціонованості дій атакуючих, які видають себе за авторизованих співробітників, керівництво тощо [6]. Основною формою СА є запит, який не потребує складних алгоритмів підготовки, та отримання відповіді від атакованого персоналу, засновуючись на психологічних принципах [4]. Найчастіше виказується інформація, яку персонал вважає неважливою, проте за її допомогою в подальшому ДІР можуть бути скомпроментовані [6]. Таким чином можна зробити висновок, що саме персонал є найбільш уразливою ланкою, якою неможливо нехтувати при оцінці стану інформаційної безпеки (ІБ) ДІР. Отже, рівень підготовленості персоналу протистояти СА є визначним чинником, який впливає на ІБ. Важливою є можливість автоматизувати процес оцінки базуючись на методологічних засадах.

У зв'язку з цим розробка методології синтезу систем оцінки рівня підготовленості персоналу протидії атакам даного класу є актуальним питанням захисту ДІР, вирішення якого є метою даної роботи.

При вирішенні завдань визначення стану ІБ інформаційних систем та розробки методів прийняття рішень використовується логіко-лінгвістичний підхід на базі теорії нечітких множин, що дозволяє формалізувати розмиті поняття та вирішити проблему математичної обробки нечіткої інформації [7].

В основі цього підходу лежить поняття лінгвістичної змінної (ЛЗ), яка є зручним засобом опису складних систем що містять параметри, подані не тільки в кількісному, але і у