

АНАЛІЗ СУЧАСНИХ СИСТЕМ УПРАВЛІННЯ КРИЗОВИМИ СИТУАЦІЯМИ

Андрій Гізун, Анна Корченко, Сергій Скворцов

Національний авіаційний університет, Україна



ГІЗУН Андрій Іванович

Рік та місце народження: 1987 рік, м. Нетішин, Хмельницька область, Україна.

Освіта: Національний авіаційний університет, 2010 рік.

Посада: асистент 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 30 наукових публікацій, серед яких наукові статті, матеріали і тези доповідей на конференціях, авторські свідоцтва.

E-mail: andriy.gizun@gmail.com



КОРЧЕНКО Анна Олександрівна, к.т.н.

Рік та місце народження: 1985 рік, м. Київ, Україна.

Освіта: Національний авіаційний університет, 2007 рік.

Посада: доцент кафедри безпеки інформаційних технологій.

Наукові інтереси: інформаційна безпека, комп'ютерна безпека, експертні системи.

Публікації: більше 40 наукових публікацій, серед яких наукові статті, підручники та навчально-методичні посібники.

E-mail: annakor@ukr.net



СКВОРЦОВ Сергій Олександрович, к.т.н.

Рік та місце народження: 1961 рік, м. Ташкент, Узбекистан.

Освіта: Київський інститут інженерів цивільної авіації, 1983 рік.

Посада: доцент кафедри безпеки інформаційних технологій.

Наукові інтереси: інформаційна безпека, технології програмування, експертні системи, штучний інтелект.

Публікації: більше 30 наукових публікацій, серед яких наукові статті, матеріали і тези доповідей на конференціях, авторські свідоцтва.

E-mail: ssamailer@gmail.com

Анотація. Концепція управління безперервністю бізнесу як перспективний напрям оперативного та стратегічного менеджменту визначає важливість захисту інформаційних ресурсів в умовах впливу кризових ситуацій. Так, поняття управління кризовими ситуаціями включає в себе їх прогнозування, ідентифікацію, реагування на негативні впливи та ліквідацію наслідків, оцінку критичності ситуації та процеси підтримки прийняття рішень і діяльності персоналу чи функціонування систем. У цій статті проведений аналіз сучасних систем управління кризовими ситуаціями, основних методів та методик, на яких вони базуються. Метою аналізу є визначення перспективних напрямів розвитку науки та техніки в даній галузі, виділення основних недоліків в існуючих системах. Дослідження охоплює як вітчизняні так і зарубіжні розробки. Основна увага приділена системам прогнозування появи кризових ситуацій, підтримки прийняття рішень і діяльності організацій в умовах невизначеності в слабоформалізованому просторі. Результати даного дослідження можуть бути використані при виборі напрямів подальших досліджень щодо розробки системи виявлення та оцінки кризових ситуацій та підтверджують доцільність і обґрунтованість застосування експертних підходів та методів нечіткої логіки.

Ключові слова: кризова ситуація, управління, система, метод, розробки, виявлення, модель, комп'ютерна програма, прогнозування, ліквідація наслідків, евакуація, системи підтримки.

Вступ

На даний момент інформаційні ресурси стають чи не найважливішим ресурсом будь-яких

підприємств, установ чи організацій усіх форм власності. Бізнес-процеси сучасних підприємств у великій мірі, а іноді і повністю залежать від

обчислювальних систем. Отже, саме IT-системи і сервіси, що забезпечують підтримку критично важливих бізнес-процесів, виявляються найбільш чутливими до впливів стихійних лих, аварій і катастроф. Для вирішення даної проблеми і розробляються плани по забезпеченню безперервності бізнесу (ЗББ).

Приблизно з 2000 року в ряді країн, головним чином у США, Великобританії, Німеччині та Канаді, проводяться щорічні слухання спеціально створених комітетів і комісій з питань стабільності і стійкості корпоративних інформаційних систем і бізнесу в цілому. Підготовлено більше десятка стандартів і специфікацій управління безпекою, що детально регламентують процедури планування та підтримки ЗББ, серед яких найбільшу популярність здобули міжнародні та національні специфікації і стандарти ISO 17799-2002, BS 25999, NIST, COOP, HIPAA Gramm-Leach-Bliley, The Expedited Funds Availability, SAS 78/94. Дані напрацювання спрямовані на реалізацію концепції управління безперервністю бізнесу (КУББ), чільне місце в якій займають процеси управління кризовими ситуаціями (КС).

Метою даного дослідження є аналіз сучасних систем та розробок в сфері управління КС, що дасть можливість виявити основні тенденції ринку даного сегменту, виявити недоліки в існуючих засобах, оцінити можливість їх застосування щодо задач різного типу, їх універсальність. Відповідно до КУББ під поняттям управління КС найбільш часто розуміється сукупність процесів з прогнозування, ідентифікації, оцінки КС, реагування та ліквідація їх наслідків. Розглянемо основні найбільш відомі вітчизняні та світові розробки в галузі управління КС.

Основна частина дослідження

Так, серед українських розробок варто відмітити ряд винаходів по забезпеченню безпеки підприємств в гірничодобувній та нафтогазовій промисловості, що ґрунтуються на контролі концентрації небезпечних речовин в свердловинах, видобутках та шахтах, а саме [1-4]. Крім того відомі системи збору інформації щодо КС і оповіщення про неї [5,6] та комп'ютеризована система контролю і визначення місця аварії силових електромереж, на основі складання карти опору і моніторингу її подальшого стану з виявленням відмінностей від еталону [7]. До даної категорії відносяться також так звані системи раннього виявлення КС (СРВКС) [8-11] та розробки з загальної реалізації антикризового менеджменту [12].

Розглянемо більш детально СРВКС, запропоновану в [11]. Корисна модель належить до систем виявлення загрози надзвичайних ситуацій техногенного характеру і забезпечення безпеки та життєдіяльності людини. Задачею корисної моделі є розширення функціональних можливостей СРВКС таким чином, щоб вона надавала можливість зберігання та аналізу стану навколишнього середовища і параметрів контрольованих сильно діючих отруйних речовин навколо об'єкта захисту, а також моделювання надзвичайних ситуацій,

максимально наближених до реальних. Поставлена задача вирішується системою, що містить метеостанцію, датчики для реєстрації параметрів поточного стану об'єкта захисту та програмно-технічний комплекс зберігання та обробки даних, що в свою чергу складається з програмно-технічного пристрою обробки даних, пристрою накопичення даних, пристрою відображення розрахункових та вимірюваних параметрів, а також додатково програмно-технічний пристрій статистичної обробки даних (надає можливість прогнозування та оцінки розвитку надзвичайної ситуації) та програмно-технічний пристрій симуляції умов надзвичайної ситуації (надає можливість змоделювати умови виникнення надзвичайної ситуації з будь-якими вихідними даними). Прототипом даної системи є винахід, описаний в [9].

Також відома СРВКС [8]. Корисна модель належить до систем, що реагують на небажані або ненормальні умови, наприклад, на злом, пожежу, ненормальну температуру, ненормальну швидкість потоку, ненормальну концентрацію газів, ненормальний рівень рідини тощо, і може бути використана для виявлення загрози КС. В основі корисної моделі поставлено задачу розширення функціональних можливостей СРВКС, яка би цілодобово з максимальною надійністю контролювала параметри технологічних процесів з наступною обробкою інформації диспетчерами за допомогою програмного забезпечення, а також мала би мінімальну вартість обміну даними, за рахунок використання передачі зашифрованої криптографічними методами інформації між системою датчик-концентратор та віддаленим сервером через мережі зв'язку з використанням протоколів пакетної передачі даних TCP/IP наземного або супутникового зв'язку. Система складається з датчиків, концентраторів, засобів зв'язку та віддаленого сервера, на якому зберігається база даних, що містить реєстр об'єктів та параметрами їх технологічних процесів, гранично допустимі значення цих параметрів, а також їх поточний стан. Датчики (газоаналізатори, рівнеміри, датчики температури, датчики тиску тощо) розміщено у техногенно небезпечних зонах, вони мають три стани – нормальний, небажаний та небезпечний, що сприяє підвищенню надійності системи в порівнянні з двозначною градацією. Таким чином в даній системі використовуються частковий випадок нечітких даних, однак значних переваг для впровадження її в слабоформалізованому середовищі це не дає, оскільки градація носить чіткий характер. Датчики підключено до концентраторів – мікропроцесорних пристроїв для збору, зберігання та шифрування одержаних даних. Концентратор періодично відправляє звіт про свій стан. В концентраторі програмується періодичність зв'язку з віддаленим сервером, а також граничне значення параметрів, при досягненні яких зв'язок відбувається позачергово. Описана система дозволяє оперативно збирати інформацію про параметри технологічних процесів з подальшою обробкою для прийняття

адекватних управлінських рішень при наявності об'єктивних та оперативних даних.

В правоохоронному документі [12] описана система для всебічного управління КС практично на більшості етапів КУББ. В основу корисної моделі поставлена задача створення інтегрованої інформаційно-аналітичної системи моніторингу зовнішнього і внутрішнього середовища підприємства, здатної за допомогою системного відбору необхідної інформації проводити комплексний аналіз ситуації і на його основі створювати варіанти моделей антикризового розвитку підприємства, що дозволяє особі, що приймає рішення (ОПР), значно полегшити розробку антикризових стратегій.

Інтегрована інформаційно-аналітична система моніторингу та моделювання антикризового розвитку підприємства містить автоматизоване робоче місце (АРМ) ОПР, підсистему управління наповненням інформації та централізовану базу даних, підсистему консолідованої інформації для ОПР, управляючу підсистему, що включає АРМ осіб, які готують стислий огляд ситуації і оцінюють перспективи її розвитку у сферах стратегічного менеджменту, маркетингу, виробничого, кадрового та фінансового менеджменту, підсистему інфраструктури менеджменту, яка включає АРМ осіб, які здійснюють цілеспрямований пошук та збір

інформації в сферах інформаційного, інноваційного, інвестиційного, проектного менеджменту, управління безпекою бізнесу та консалтингу, її структурування та зберігання, попередню обробку і моніторинг інформації, яка необхідна фахівцям управляючої підсистеми.

Інтегрована інформаційно-аналітична система моніторингу та моделювання антикризового розвитку підприємства має централізовану базу даних, яка є спеціалізованою антикризовою базою даних, що містить актуальну і архівну інформацію з стратегічного менеджменту, маркетингу, виробничого, кадрового та фінансового менеджменту, інформаційного, інноваційного, інвестиційного, проектного менеджменту, управління безпекою бізнесу і консалтингу, що сформована фахівцями відповідних підрозділів і відповідає критеріям антикризового розвитку. Вона має також підсистему консолідованої інформації для ОПР, яка представляє блок інтегрованої інформації, що містить агреговані дані та прогнози розвитку ситуації у зовнішньому і внутрішньому середовищі, пропозиції відносно подальших дій, що дає можливість розробляти моделі антикризового розвитку. загальну структурну схему наповнення підсистеми консолідованої антикризової інформації, яка спрямовується на АРМ ОПР, зображено на Рис. 1 [12].

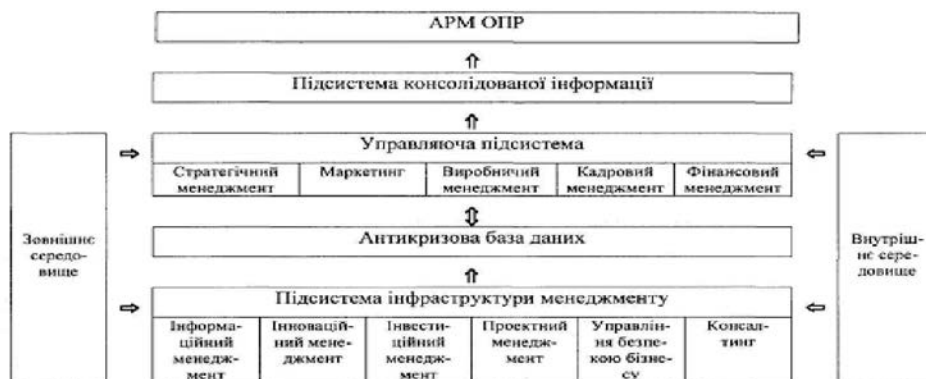


Рис. 1. Структурна схема наповнення підсистеми консолідованої антикризової інформації

Відомий спосіб прогнозування викидо-небезпечності масиву гірських порід, який включає аналіз змін сили тяжіння в конкретній зоні масиву, облік геологічних порушень, розрахунок несприятливих часових інтервалів [13]. Однак даний спосіб не забезпечує можливість прогнозування конкретного місця і часу будь-якої аварії в шахті.

Автори роботи [14] стверджують, що всі матеріальні об'єкти мають свою тривимірну полярність. Гірничі машини, транспортні засоби, різні механізми, електрообладнання та інші об'єкти при безаварійному стані мають нормальну полярність. Зміна енерго-інформаційного стану технічного об'єкта може привести до зміни полярності і аварій. Ретроспективний аналіз фантомів технічних систем, які опинилися в аваріях, показав, що всі вони мали зворотну полярність [15].

На основі квантового підходу ними розроблений спосіб прогнозування аварійних ситуацій в шахтах [2]. Спосіб здійснюється шляхом

дистанційного визначення і контролю інтегральних параметрів полярності і напрямку обертання локального торсійного поля системи гірський масив - видобуток. Для аналізу стану безпеки окремих виробок, ділянок або шахт в цілому використовують їх моделі, план гірничих робіт, технологічні схеми, що їх характеризують. Виявлено, що поєднання нормального розподілу знаків полярності з правостороннім торсійним полем означає безаварійне стан об'єкта. А зворотна полярність в поєднанні з лівостороннім торсійним полем означає, що аварійна ситуація виникла. Між нормальним і аварійним станом об'єкта існує перехідний стан, коли полярність об'єкта змінена на зворотну при збереженні правостороннього торсійного поля.

Момент виникнення аварійної ситуації визначають відповідно до виразу $m_a = m_c + A\Gamma_c \pm A\Gamma_\theta$, де m_a - момент виникнення аварійної ситуації в часі; m_c - момент появи сигналів про можливу аварійної ситуації; $A\Gamma_c$ - тривалість загрозливого стану об'єкта;

$A_{г}$ - середньостатистичне відхилення від значення $A_{гc}$. Момент появи сигналу про можливу аварійної ситуації визначають з виразу $m_c = m_m - A_{m_p}$, де m_m - момент поточного часу, коли був виявлений сигнал про можливу аварійної ситуації; A_{m_p} - затримка прийомом оператором аварійного сигналу.

Контроль за станом гірських масивів і виробок з даного способу здійснюється шляхом періодичного тестування їх методом біолокації. Періодичність тестування визначають з таким розрахунком, щоб залишався час для виконання превентивних заходів проти можливої аварійної ситуації або аварії. Спочатку тестують систему в цілому, наприклад - шахту. Потім тестують окремі ділянки і виробки. Аналіз аварій, що сталися на шахтах Донбасу, показав, що сигнал про можливу аварійну ситуацію з'являється не тільки на аварійній ділянці, а й по шахті в цілому, тобто система за допомогою торсіонних полів і випромінювань відгукується на зміни в її підсистемах і елементах.

Перевагою квантового способу прогнозування аварійних ситуацій в підземних виробках є можливість дистанційного та оперативного отримання інформації про можливу аварійну ситуацію до її виникнення. Спосіб дозволяє визначити місце і час аварії, в тому числі: раптові викиди вугілля, породи і газу; спалахи і вибухи газу; пожежі; обвалення породи; аварії на гірничодобувному, гірничо-транспортного і електротехнічному устаткуванні; травмування гірників; теплові удари та інше [14]. Даний метод є повністю універсальним і може використовуватися не лише в гірничій галузі. Однак для використання даного методу на сьогоднішній день не сформована відповідна теоретико-доказова база.

Дослідження російського сегменту ринку програмних продуктів забезпечення безперервності бізнесу показало, що виявлені в публічному доступі продукти призначені для моделювання розвитку та наслідків надзвичайних ситуацій конкретного типу (Автоматизована система підтримки прийняття рішень з ліквідації надзвичайних ситуацій на хімічно небезпечних об'єктах, Програма «АХОВ», Програма «ТОКСІ», Програма «АМІАК», Програма «ЕКСПРЕС-ОЦІНКА», Програмний комплекс ТОКСІ + (Версія 4.1) («ТОКСІ + RISK»), Програмний комплекс з розрахунку наслідків аварій ТОКСІ +, Модуль «Ризик НС (оператор)» - ArcMap, ArcScene, «РизЕкс - 2» - Дослідницький програмний комплекс моделювання аварій і оцінки ризику. Модуль «Розсіювання НХР. РД52»), що може бути використано в колекції сценаріїв ліквідації критичних ситуацій, але не для комплексної підтримки управління критичними ситуаціями.

З метою оптимізації процесів інформаційної підтримки управління кризовими ситуаціями в [16] розроблена стратифікована модель управління промисловою безпекою організації / підприємства. Нормативний страт моделі насичений відомостями про технології, підходи, методики ліквідації критичних, у тому числі надзвичайних, ситуацій, сконцентрованими в нормативних документах федерального і галузевого рівнів. У структурі

програмного комплексу програмного страта моделі управління кризовими ситуаціями ключовими об'єктами є підприємство / організація, небезпечний виробничий об'єкт, технологічний процес, речовина / небезпечна речовина, проблема / збій / аварійна ситуація. Надзвичайна ситуація характеризується наступною інформацією: можливі причини аварії; система протиаварійного захисту; відомості про заходи щодо локалізації та ліквідації наслідків аварій на декларованому небезпечному виробничому об'єкті і т.д.

Для забезпечення можливості прогнозування виникнення аварійної ситуації експерт задає для кожної неполадки два вектора ймовірностей. Перший вектор вказується за допомогою значень в діапазоні від 0 до 1 і визначає ймовірність того, що відбудеться надзвичайна ситуація з певної групи сценаріїв аварій. Другий вектор містить значення ймовірностей того, що станеться конкретна аварія з групи сценаріїв надзвичайної ситуації. Висновок про найбільш вірогідну групу сценаріїв аварії робиться за формулою Байеса. Спочатку ймовірність кожної альтернативи задається як результат ділення 1 на кількість груп сценаріїв надзвичайних ситуацій або аварій відповідно. Перемноживши, по Байесу, вектора ймовірностей всіх вказаних користувачем неполадок (проблем), отримується вектор, що характеризує найбільш ймовірні групу сценаріїв і аварію, її значення ймовірності буде максимальним [16] Запропонована система відповідає вимогам універсальності і за умов спеціального налаштування може бути використана в ІБ.

Доступні для аналізу сучасні методи та технології підтримки дій диспетчера в основному спрямовані на створення апаратної підтримки ранньої стадії виявлення аварій [17] і систем оповіщення [18]. Наприклад, комплекс автоматизованих систем раннього виявлення надзвичайних ситуацій та оповіщення, що розробляється підприємствами ТОВ ВНФ «Елон-ТТ» (м. Харків), ТОВ НВП «Озон-С» (м. Дніпропетровськ) та ТОВ «Оптіма-Комплекс» (м. Запоріжжя), призначений для реалізації наступних операцій: раннього виявлення загрози виникнення надзвичайних ситуацій (контроль до критичних параметрів); виявлення надзвичайних ситуацій (контроль критичних параметрів); оповіщення працюючого персоналу та інших осіб, які перебувають на території ВАТ «Запоріжжкокс», керівного складу, відповідальних посадових осіб територіальних органів МНС та цивільного захисту населення, органів виконавчої влади про загрозу або виникнення КС. Даний комплекс задовольняє вимогам наказу МНС України № 288 і може бути базовим для підтримки дій диспетчера підприємства, але цей комплекс не вирішує завдання прогнозування наслідків аварії з урахуванням поточних реальних умов. До локальних систем оповіщення, керованим диспетчером, відносяться такі системи, як комплекс централізованого оповіщення «Співак» або комплекс централізованого оповіщення «Зоря» [18]. Дані системи виконують тільки частину функцій, покладених на диспетчера і

пов'язаних з автоматичним сповіщенням. Основним недоліком цих систем є неможливість динамічного формування таблиць оповіщення і повна відсутність підтримки дій диспетчера в прогнозуванні та координації служб при ліквідації наслідків аварії. У Росії останнім часом створюється загальноросійська комплексна система інформування та оповіщення населення в місцях масового перебування людей (ОКСІОН) - комплекс сучасних систем спостереження, інформування та оповіщення, що розробляється в рамках Федеральної цільової програми «Зниження ризиків і пом'якшення наслідків надзвичайних ситуацій природного і техногенного характеру в Російській Федерації до 2010 року». До середини 2010 року збудовано та введено в експлуатацію всього 520 термінальних комплексів ОКСІОН. Весь комплекс знаходиться в управлінні ГУ ШЦ "ОКСІОН" - (Державна установа: «Інформаційний центр Загальноросійської комплексної системи інформування та оповіщення населення в місцях масового перебування») [19]. Цей комплекс має структуру і функції загальнодержавного рівня із застосуванням в регіональному масштабі. Незважаючи на складне і множинне функціональне і програмно-апаратне забезпечення, вхідні дані такої системи не можуть бути суміщені з даними конкретного підприємства, що дозволяють встановити масштаб аварії і провести достовірний прогноз. У всякому разі в такому комплексі немає підтримки дій диспетчера та формування динамічних таблиць оповіщення.

Метод прогнозування наслідків та модель автоматизованої системи підтримки дій диспетчера небезпечного виробництва при виникненні аварійних ситуацій, запропонований в [20], базуються на розгляді складної фізичної системи (СФС), що включає в себе небезпечне виробництво, диспетчерську службу, апаратну систему контролю технічного стану виробництва як єдину інформаційну структуру.

Математична модель процесу прийняття рішень ОПР при виникненні і розвитку аварій на небезпечному виробництві заснована на послідовності перетворень. Ця модель представлена кортежем виду $D = \langle \bar{T}, \bar{P}, \bar{M}, \bar{E}, \bar{R} \rangle$, де \bar{T} - вектор параметрів стану засобів технічного забезпечення оповіщення та визначення погодних умов; \bar{P} - вектор параметрів, що визначають розташування джерел небезпеки в метричному просторі; \bar{M} - вектор параметрів, що характеризують масштаби і величини параметрів аварійного процесу; \bar{E} - вектор текстових семантичних параметрів, що визначають тип аварійної події; $R = [R_d, R_s]^T$ - вектор величин параметрів, що характеризують дії диспетчера R_d в різних ситуаціях і список оповіщення R_s , сформований динамічно на основі даних прогнозу.

Таким чином, необхідно в заданий час провести: введення початкової інформації; виконати математичне моделювання несприятливих фізичних процесів; провести аналіз отриманих даних і виділити об'єкти, для яких прогнозовані наслідки

перевищують прийнятний рівень $\bar{M}_k > \bar{M}_{\text{прием}}$, де $\bar{M}_{\text{прием}}$ - вектор значень прийнятних наслідків; визначити значення вектора параметрів \bar{R} , що характеризують реакцію СФС на вплив; виконати операції інформаційного забезпечення засобів автосповіщення. Передбачається, що в процесі роботи виробництва в аварійній ситуації за допомогою програмних засобів ведеться моніторинг стану СФС в реальному часі [20].

Автоматизований програмно-апаратний комплекс (АПАК), розроблений на основі даної моделі, складається з наступних складових:

- Програмний модуль, що містить засоби моделювання несприятливих фізичних процесів і дозволяє проводити попередній аналіз і прогнозування розмірів областей і значень параметрів вражаючих факторів для зазначених видів загроз;

- Програмний модуль, що дозволяє формувати, доповнювати і редагувати базу даних, що містить інформацію про джерела небезпеки, види загроз, обслуговуючий персонал, служби і об'єкти відповідальності;

- Апаратна група, що включає в себе: комплекс датчиків, локальну мережу комп'ютерів, програмне забезпечення для збору, обробки і відображення інформації, автоматичну цифрову метеостанцію, локальну систему оповіщення та АТС, керовані цифровими комутуваними засобами [20].

На підставі проведеного аналізу засобами програмного забезпечення формується база даних (БД). У таблицях БД вказуються місця розташування джерел небезпеки. Далі здійснюється прив'язка аварійної ділянки до об'єктних карт, виконаних у реальному масштабі; задаються растрові і векторні карти для відображення; визначаються види загроз, реалізація яких можлива при даному джерелі небезпеки; вводяться дані, необхідні для виконання математичного моделювання та визначення параметрів для прогнозу наслідків аварії. У підсумку формуються таблиці, що містять вимоги щодо обов'язкового оприлюднення і дій диспетчера в умовах КС.

Важливою частиною АПАК підтримки прийняття рішень диспетчерської служби при виникненні і розвитку аварій є достовірність та інформаційна повнота прогнозу. Прогноз заснований на використанні даних про реальний стан навколишнього середовища в момент виникнення аварії та наявних у розпорядженні математичних моделей несприятливих фізичних процесів.

Відома система для зменшення збитків та руйнувань в результаті стихійних лих [21]. Основною метою розглянутої системи є зменшення пошкоджень будівлі після землетрусу. Так система призначена для управління зовнішніми комунікаціями надання комунальних послуг, такими як водо-, газо- та електропостачання до окремої будівлі, що знаходиться в зоні ураження. До складу системи входять набори датчиків 3-ьох типів: сенсор виявлення землетрусу, датчики контролю

стану приміщень в будівлі (наявність/відсутність затоплень, пожежі, розривів трубопроводів тощо) та датчики контролю постачання комунальних послуг. При отриманні сигналу щодо можливості чи факту землетрусу система перевіряє датчики контролю приміщень на наявність пошкоджень і передає сигнал щодо прийняття рішення про відключення або залишення в працюючому стані комунікацій. Наприклад, якщо в результаті руйнувань, спричинених землетрусом, в будівлі виникає пожежа, система приймає рішення про відключення газопостачання або при наявності розривів в газопроводах система терміново відключає електроживлення в будинку з метою унеможливлення появи пожежі. Більш того, система ціленаправлено не відключає комунікації, які можуть посприяти усуненню негативних чинників під час КС, наприклад, при пожежі система водопостачання залишається працювати в повному об'ємі. Перевірки системою стану будівлі періодично повторюються до усунення всіх негативних факторів. При кожній перевірці стан комунікацій перевіряється і може бути змінений. Рішення

системи здійснюються в відповідності до набору правил, зображених на рис. 2, в базі даних, які можуть коректуватися в подальшому.

У правоохоронному документі США [22] описані апарат та метод прогнозування стихійних лих. В основу апарату прогнозування стихійних лих входять комп'ютер, мінімальна конфігурація якого складає наявність процесора і пам'яті, що містить програму функціонування апарату прогнозування, а також базу даних, в якій записані різноманітні сценарії КС. Крім того апарат отримує дані з метеорологічної станції, дані прогнозу погоди, землетрусів тощо, звіти щодо надзвичайних ситуацій та КС, а також має зв'язок з супутниковим сателітом, що передає картографічну інформацію та географічні координати КС через мережу Інтернет, і різними адміністративними органами, такими як міністерства. Типова структура описаного апарату наведена на рис. 3. Виконуючи свої функції комп'ютер посилає запит щодо надання супутникових знімків території, визначає географічні координати місця можливого стихійного лиха, вираховує індекс ризику лиха.

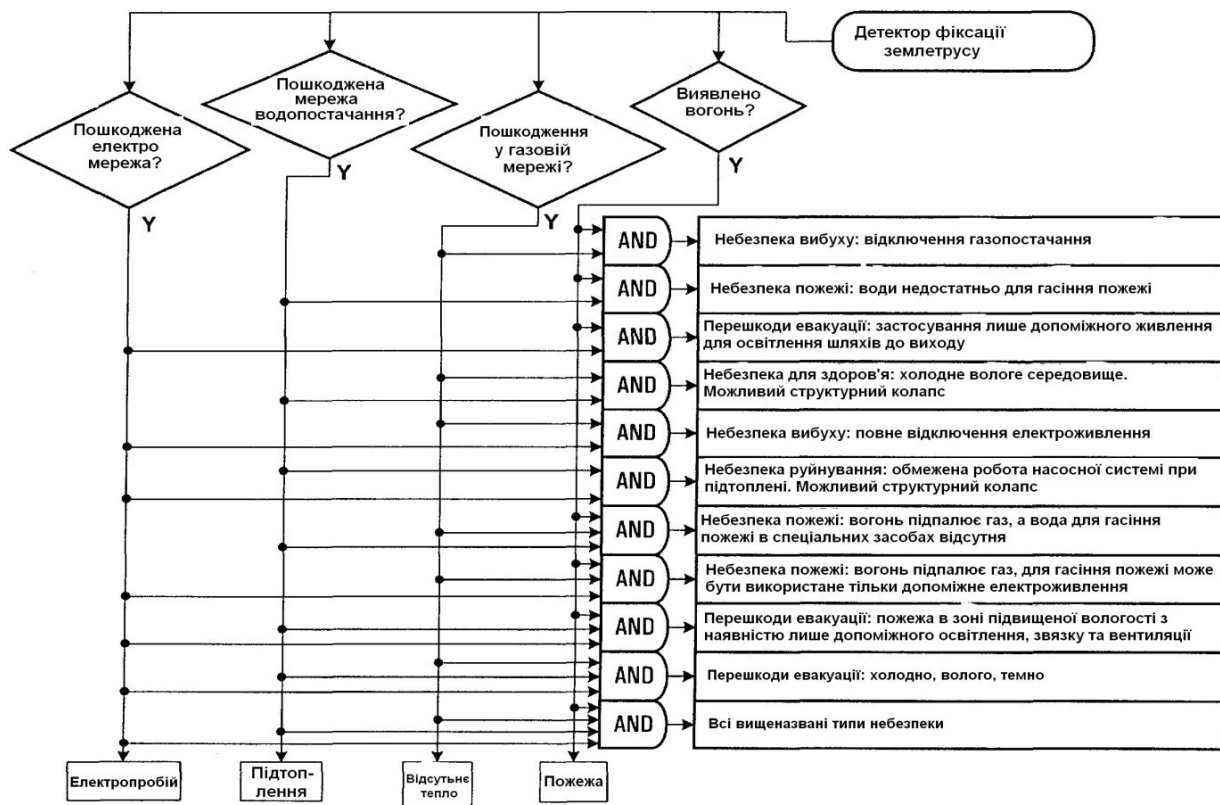


Рис. 2. Схематичне зображення набору правил контролю комунікацій

Для здійснення прогнозів метеорологічні дані передаються через мережу від метеорологічних центрів або приватних метеорологічних компаній, таких як автоматизована метеорологічна система отримання і накопичування даних (AMeDAS). До них відносяться інформація щодо цунамі, землетрусів, вулканічної діяльності, штормових попереджень, довгострокові прогнози, матеріали спостережень, спеціальна погодна інформація, авіаційні погодні матеріали і т.п. Крім того, також

через мережу передаються дані прогнозу погоди та відомості з сейсмічних станцій.

Метод прогнозування стихійних лих полягає в наступних кроках: 1) отримання та аналіз метеоданих, 2) у випадку якщо вони перевищують встановлені порогові значення робиться запит до супутника на отримання картографічної інформації, 3) отримані супутникові дані порівнюються з стандартними і пікселі, в яких поточні значення менші або рівні пороговим видаляються, тобто визначається область ураження,

4) відправляється аварійне повідомлення, в якому вказано тип та місце можливого стихійного лиха, 5) реєструється факт відправлення аварійної пошти та її вміст.

Подібна система, описана в [23], для прогнозування землетрусів з використанням сейсмічних вимірювань вираховує координати його епіцентру, силу землетрусу та зону враження. Отримані дані передаються на термінали системи.

Описаний в [24] статистично-детермінований підхід щодо прогнозування стихійного лиха, використовуючи історичні та статистичні дані щодо фіксації в регіоні ураганів, шквальних вітрів, смерчів, а також математичний апарат теорії імовірності та математичні розподіли (Гауса, Пуассона), здійснює прогнозування та оцінку ймовірності появи урагану на певній території.

В [25] розглянуті метод і апарат для попередження КС, що за своєю суттю може бути названий «Евакуаційним гідом». На певній території різних масштабів (будинки, готель, торговельно-

розважальний центр) встановлюються датчики, що фіксують появу тої чи іншої КС, переважно орієнтовані на пожежу. В якості датчиків можуть використовуватися температурні датчики, датчики емісії диму, вологі тощо. У випадку появи кризового чинника, тобто виникнення КС, датчики передають на сервер відомості щодо їх місцезнаходження. Опрацювавши отримані дані сервер формує оптимальні маршрути евакуації в онлайн-режимі, враховуючи всі можливі зміни в розвитку ситуації, що включають напрями руху, відстані, розміщення перешкод. Сформований план евакуації передається на мобільні термінали жителів/персоналу, в тому числі в якості терміналів можуть використовуватися особисті мобільні телефони, комунікатори, цифрові асистенти PDA, приймачі чи інші гаджети. Крім того система здатна управляти електронними засобами, наприклад, блокувати/відкривати електронні замки, двері. Зв'язок між датчиками, сервером та мобільними терміналами здійснюється через радіоканал.

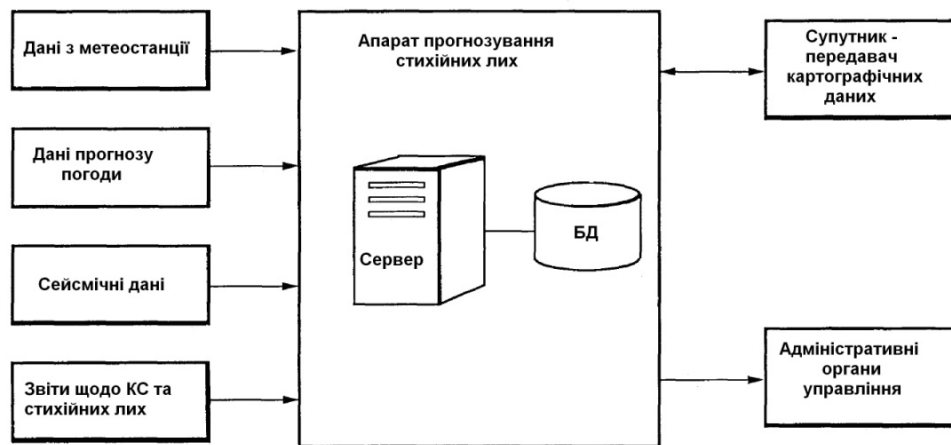


Рис. 3. Типова структура апарату прогнозування стихійних лих

Аналогічним є пристрій, права на якого підтверджені документом [26]. Він визначений автором як динамічний план дій на випадок КС сімейного типу. Користувач, оператор чи урядові агенції можуть генерувати повідомлення про КС, їх масштаб та вказівки необхідних дій, що відсилаються особам в ареалі враження. До того ж можуть бути використані шаблони типових КС і дій при них, що передаються мешканцям районів історично схильним до них. Система дозволяє підтримувати зв'язок членам сім'ї між собою та з оператором до, під час і після КС.

Схожим за призначенням та принципом дії є спосіб управління та апарат контролю за системою протидії лиху [27]. У випадку виникнення КС система підпорядковує собі контроль за радіоканалом в зоні враження і використовує його для передачі інформації щодо ситуації та її статусу. Повідомлення передаються через мережі мобільної комунікації та стаціонарні мережі на користувацькі термінали в зоні розповсюдження КС. Є можливість відправляти швидкі повідомлення, задавати їх пріоритет в радіоканалі, блокувати непідтвержені повідомлення, Користувач може підписатися на оновлення щодо ситуації в реальному часі,

створювати, передавати і отримувати повідомлень 5-ти видів: дані статусу КС, текстові коментарі, зображення місця КС, відео з місця локалізації КС, голосові повідомлення.

Відомі метод та апарат [28] для визначення ймовірності КС в сфері комунікацій, а саме в мережі чи її частині, та збитків, принесених ними. Тобто він напряму використовується в питаннях менеджменту ІБ, але сфера його використання досить обмежена. Апарат та метод можуть бути використані як для окремих елементів мережі, множини елементів мережі, всієї мережі та множини мереж.

Визначення очікуваного впливу різних КС на систему комунікацій і її різні частини здійснюється з використанням моделі аналізу КС, що є комбінацією моделі мережі і моделі КС. Модель КС охоплює різні типи ситуацій згідно їх структури (представлення специфічних категорій моделлю Пуассона) і параметрів. Серед специфічних категорій виділені стихійні лиха, технічні аварії або ситуації, пов'язані з людським фактором. До стихійних лих розробники відносять землетруси, торнадо, паводки, до технічних – відмови електроживлення, витoki газу, а до людських – тероризм, вандалізм тощо. Взаємозв'язок параметрів цих моделей описується у

вигляді матриці. Так, одне з основних місць займає матриця ймовірності впливу КС D на елемент системи E

$$\begin{bmatrix} Parametr(Pd) & E1 & \dots & EN \\ D1 & Pd(E1, D1) & \dots & Pd(EN, D1) \\ \dots & \dots & \dots & \dots \\ DE & Pd(E1, DE) & \dots & Pd(EN, DE) \end{bmatrix}$$

Модель аналізу КС включає в себе параметри для визначення кількості ймовірності того чи іншого пошкодження в різних сегментах мережі. Так, ймовірність виникнення КС D дану кількість раз (a) протягом періоду часу T в елементі мережі E визначається як:

$$Pd_{(Ei, Dj)}(a, T) = e^{-Rd_{(Ei, Dj)} * Ph_{(Ei, Dj)} * T} \left[\frac{(Rd_{(Ei, Dj)} * Ph_{(Ei, Dj)} * T)^a}{a!} \right],$$

де Rd – норма виникнення Кс, Ph – ймовірність, що КС вплине на елемент E.

Також модель аналізу КС використовується для визначення її впливу на мережу. Наприклад, до параметрів впливу відносять вартість заміни пошкоджених елементів мережі, вартість переривання надання послуг, втрату доходів, штрафи SLA і інші.

В методі пропонується вираховувати вартість заміни пошкодженого обладнання елементу мережі E внаслідок впливу КС D як $Gbm_{(Ei, Dj)} = Pg_{(Ei, Dj)} * Pk_{(Ei, Dj)} * Ce_{(Ei, Dj)}$, де Pg – параметр пошкодження основного обладнання, Pk – ймовірність пошкодження елементу мережі, Ce – вартість відновлення елементів мережі. А вартість переривання обслуговування елемента мережі як $Sbm_{(Ei, Dj)} = Sl_{(Ei, Dj)} * Pk_{(Ei, Dj)} * Si_{(Ei, Dj)} * MTTR_{(Ei, Dj)}$, де Sl – вартість переривання обслуговування, Si – індикатор переривання обслуговування мережевого елемента, $MTTR$ – середній час відновлення елемента мережі. Таким чином вартість впливу КС на мережу становить $Cbm_{(Ei, Dj)} = Gbm_{(Ei, Dj)} + Sbm_{(Ei, Dj)}$.

Розробка [29] включає в себе систему, метод та комп'ютерну програму для оцінки ризику КС в IT-інфраструктурі. Запропонований метод і система ґрунтуються на теорії небезпек. Вхідними даними в даному випадку є інформація про час і серйозність попередніх інцидентів. На основі залежності між попередніми інцидентами (відповідним часом виникнення та силою негативного впливу), використовуючи статистичні залежності між ними, що описуються поліномом Чебишева

$$P_n(x) = \sum_{i=1}^n (y_i \prod_{j=1}^n \frac{(x - x_j)}{(x_i - x_j)}),$$

здійснюється оцінка ризику майбутніх інцидентів та їх величини, тобто можливий час виникнення і серйозність наслідків майбутньої КС.

Метод оцінки ризику майбутньої КС в IT-інфраструктурі включає наступні кроки: 1) ідентифікація часу попередніх КС, 2) визначення рівня серйозності (величини впливу) попередніх КС, 3) побудова функції полінома Чебишева на основі співвідношення отриманих на етапах 1-2 даних щодо попередніх КС і 4) оцінка ризику майбутніх КС в IT-інфраструктурі. Реалізована система вміщує в собі

відповідні засоби для реалізації кроків вищеописаного методу.

Відома система прогнозування катастроф або КС [30] ґрунтується на методах, що оперують поняттями нормальності та ненормальності на основі порівняння поточних значень з пороговими значеннями. Система прогнозування КС складається власне з апарату прогнозування, що збирає, обробляє, зберігає, приймає та передає сигнали ненормальності, та множини мобільних радіоапаратів комунікації (термінали), які збирають та передають інформацію щодо ситуації до центрального апарату через мережу радіозв'язку. Мобільні радіоапарати вміщують в собі модуль визначення місцезнаходження, модуль виявлення ненормального сигналу (тут отримавши електромагнітний сигнал з навколишнього середовища датчик визначає ненормальний сигнал і формує сигнал виявлення ненормальності), 1-ий модуль комунікацій, що передає актуальне місцезнаходження на апарат управління місцезнаходженням, а сигнал виявлення ненормальності – до апарату прогнозування, а також здійснює зворотний зв'язок. Апарат управління місцезнаходженням фіксує і контролює положення і географічні координати кожного мобільного терміналу. Центральний апарат прогнозування складається з 2-ого модуля комунікацій (отримує сигнали ненормальності та інформацію щодо місцезнаходження від множини мобільних терміналів і у відповідь передає сформовану інформацію щодо КС назад) та модуля прогнозування КС, який збирає та аналізує сигнали ненормальності і прогнозує виникнення стихійного лиха, визначає області ураження та формує аварійні повідомлення. До складу модуля прогнозування входить блок зберігання порогового значення, з яким порівнюється електромагнітний сигнал (визначається середнє та максимальне значення рівня сигналу), і, власне, блок порівняння, що продукує сигнал виявлення КС у випадку якщо рівень електромагнітного сигналу перевищує рівень порогу. Тут приймається рішення щодо прогнозу КС. Крім того, до складу системи прогнозування КС входить модуль приведення в стан готовності, в якому формуються звукові, вібраційні, світлові, графічні та відеосигнали, пов'язані з КС та її перебігом. Система є достатньо універсальною з точки зору її використання щодо різних КС, але не підтримує всі етапи КУББ.

Метод і система формування планів реагування на КС (по суті планів ЗББ) та оцінки впливів на бізнес, описана в [31] поєднують в собі функції прогнозування динаміки КС і планування бізнесу, полегшуючи обчислення фізичних і інших ефектів від КС в грошовому виразі. А також дозволяють користувачу оцінити витрати на реалізацію різних окремих планів ЗББ чи їх комбінацій, вибрати оптимальний набір заходів. Це досягається через системний аналіз багатьох сценаріїв КС, за рахунок аналізу потенційного впливу КС на ділові операції, фізичну і IT-інфраструктуру, персонал та клієнтів, ділових

партнерів, витрати на сервісне обслуговування. Система може бути використана користувачем як локально так і через мережу, в тому числі Інтернет.

Система складається з таких складових (рис. 4): калькулятор динаміки КС, калькулятор

інфраструктурних чинників, калькулятор економічних чинників, калькулятор поведінкових чинників і калькулятор ефективності бізнесу та блок введення вхідних параметрів та корегування планів реагування.



Рис. 4. Структура системи формування планів ЗББ та оцінки впливів КС

Таким чином система і метод з використанням комп'ютерних потужностей проводить інструктаж щодо ВІА і ризиків, пов'язаних з КС. До вихідних функцій системи відносяться: 1) обчислення матеріальної або глобальної динаміки КС, 2) обчислення психологічних, економічних і/або фізичних впливів КС, включаючи, але не обмежуючись потенційними взаємозалежностями між цими чинниками і динамікою КС, 3) обчислення фінансових і експлуатаційних впливів КС, 4) оцінка ефектів різних планів реагування і витрат на їх виконання, 5) оптимізація планів відносно однієї чи декількох бізнес-цілей.

В процесі роботи системи використовуються методи моделювання для того, щоб врахувати глобальну динаміку КС, виміряти психологічні, фізичні та економічні впливи на підприємстві і ефекти від впровадження різних планів ЗББ, наприклад зберігання резервного інвентарю та обладнання, розподіл вакцин, навчання та інструктажі персоналу, договори з постачальниками, закриття окремих ланок підприємства та евакуація працівників. Для характеристики планів реагування на КС використовують ряд параметрів, а саме рівень

запасів інвентарю в резерві, ефективність евакуації, ефективність вакцин, часові характеристики виконання плану УББ (період старту і закінчення) тощо. Оптимізації планів реагування може здійснюватися шляхом: 1) модифікації структури залежностей між постачальниками, партнерами та клієнтами підприємства, фізичною і ІТ-інфраструктурою, 2) модифікації детальних параметрів планів, 3) модифікації тривалості планів. Сутність цих змін може бути визначена через проект одного чи декількох експериментів, який систематично досліджує вказані параметри і ідентифікують їх комбінацію оптимальну для роботи підприємства відносно тієї чи іншої бізнес-цілі. Плани реагування на КС, якими підприємство не керує (наприклад, державні, міністерські плани) можуть задаватися як незмінні. При введенні відповідних параметрів така система може бути використана в менеджменті ІБ.

Детально розглянувши описані засоби, визначимо основні параметри їх функціонування, вхідні і вихідні дані, принципи роботи та основні галузі застосування. Отримані результати наведемо в вигляді таблиці 1 та таблиці 2.

Таблиця 1

Порівняльний аналіз сучасних систем управління кризовими ситуаціями

Засіб	Вхідні дані	Принцип функціонування	Вихідні дані	Галузь застосування/ Використання в ІТ
Система раннього виявлення надзвичайних ситуацій [11] (Україна)	Статистичні дані метеоумов, параметри контрольованих отруйних речовин (концентрація і т.п.)	Оперативний режим: компараторний принцип. Імітаційний режим: моделювання на основі статистичних даних	Сигналізація щодо КС, прогноз розвитку та динаміки	Промислова безпека / не використовується
Система раннього виявлення надзвичайних ситуацій [8] (Україна)	Параметри датчиків в техногенно небезпечних зонах	Компараторний принцип, теорія прийняття рішень	Контроль технологічних процесів, підтримка прийняття рішень в умовах КС	Промислова безпека / не використовується

Продовження табл. 1

Інтегрована інформаційно-аналітична система моніторингу та моделювання антикризового розвитку підприємства [12] (Україна)	Актуальна і архівна інформація щодо управління підприємством (менеджмент, маркетинг, фінансові показники, безпеки тощо).	Аналітична та консолідована обробка інформації, теорія прийняття рішень, експертні підходи	Прогноз розвитку ситуації, розробка рекомендацій, моделювання варіантів антикризового розвитку	Менеджмент / частково використовується
Спосіб прогнозування викидонебезпечності масиву гірських порід [13] (Україна)	Геологічні дані, вимірювання сили тяжіння	Аналіз зміни сили тяжіння, геологічних порушень Статистичні характеристики	Прогноз викидів в гірських масивах	Гірничодобувна галузь / не використовується
Спосіб прогнозування аварійних ситуацій в підземних гірничих виробках [2, 14] (Україна)	Інтегральні параметри полярності і напрямку обертання локального торсіонного поля	Теорія торсіонних полів, квантові методи вимірювання	Прогнозування КС в шахтах	Гірничодобувна галузь / не використовується
Програмний страт моделі управління кризовими ситуаціями [16] (РФ)	Параметри технологічних процесів, вектор ймовірностей реалізації сценаріїв, вектор ймовірностей реалізації аварій	Байєсівські мережі, теорія ймовірностей	Прогноз загальної ймовірності реалізації КС, моделі ліквідації наслідків	Менеджмент, промислова безпека / не використовується
Автоматизована система підтримки дій диспетчера небезпечно виробництва при виникненні аварійних ситуацій [20] (РФ)	Місця розташування джерел небезпеки, прив'язка аварійної ділянки до об'єктних карт, види загроз, дані про ландшафтні, погодні умови	Математична модель прийняття рішень в квантній фізичній системі	Відомості про небезпечні зони, ступені загрози в прилеглому просторі; кількість і місця знаходження людей, що потрапляють в зону ураження, заздалегідь підготовлені дані про можливі шляхи евакуації	Менеджмент, промислова безпека, безпека населення / не використовується
System for reducing disaster damage – Система для зменшення збитків та руйнувань в результаті стихійних лих [21] (США)	Дані сенсорів виявлення землетрусу, датчиків контролю стану приміщень в будівлі та датчиків контролю постачання комунальних послуг	Системний аналіз стану контрольованого об'єкта, теорія прийняття рішень, компараторний принцип	Контроль комунікацій в приміщенні під час КС	Цивільний захист населення під час землетрусів / не використовується
Disaster predicting method, disaster predicting apparatus, disaster predicting program – Апарат прогнозування стихійних лих [22] (США)	Сценарії КС, метеодані, звіти щодо КС, картографічні дані з супутника	Обробка статистичних даних, компараторний принцип, обробка растрового зображення	Обчислення рівня ризику стихійних лих, визначення географічних координат. Сигналізація	Цивільний захист населення від природних стихійних лих / не використовується
Statistical-deterministic approach to natural disaster prediction – Статистично-детермінований підхід щодо прогнозування стихійного лиха [24] (США)	Статистичні та історичні дані метеорологічних спостережень	Математичний апарат теорії ймовірності та статистичних розподілів (Гауса, Пуассона)	Прогнозування стихійних лих, сигналізація	
Method and apparatus for disaster prevention – «Евакуаційний гід» [25] (США)	Параметри датчиків контролю стану приміщень (температурні датчики, датчики емісії диму, вологи)	Компараторний принцип, використання наборів сценаріїв поведінки	Виявлення КС. Сигналізація, рекомендації та контроль за евакуацією	Цивільний захист населення в громадських та розважальних місцях, місцях проживання / не використовується
Dynamic emergency disaster plan – Динамічний план дій на випадок КС [26] (США)	Сигнал про КС	Статистичні та історичні дані, використання наборів сценаріїв поведінки, моделювання	Сигналізація, рекомендації та контроль за евакуацією, рекомендовані плани дій в умовах КС	

Закінчення табл. 1

Method and apparatus for quantifying an impact of a disaster on a network – Метод та апарат для визначення впливу КС на комп'ютерні мережі [28] (США)	Вартість обладнання та відновлених робіт, вартість переривання обслуговування (встановлюється експертом), <i>MTTR</i> – середній час відновлення	Теорія ймовірності, теорія небезпек, статистичні розподіли Пуасона, системний аналіз об'єктів, методики аналізу впливу на бізнес	Вартість впливу КС на комп'ютерну мережу, зокрема ІТ інфраструктуру	ІТ-інфраструктура, відновлення бізнес-процесів після КС в КУББ / використовується
System, method and program for estimating risk of disaster in infrastructure – Система, метод та комп'ютерна програма для оцінки ризику КС в ІТ-інфраструктурі [29] (США)	Інформація про час і серйозність попередніх інцидентів	Теорія небезпек, статистичні залежності між попередніми і майбутніми інцидентами (задаються поліномом Чебишева)	Оцінка ризику майбутніх інцидентів та їх величини (серйозності наслідків)	ІТ-інфраструктура, прогнозування та оцінка ризиків, КУББ / використовується
Disaster prediction system – Система прогнозування КС (катастроф) [30] (США)	Парметри датчиків контролю навколишнього середовища у вигляді електромагнітних сигналів	Теорія небезпек, апарат еталонних значень (нормальності / ненормальності), компараторний принцип	Прогноз виникнення стихійного лиха, визначення області ураження. Сигналізація (аварійні повідомлення)	Менеджмент, промислова та цивільна безпека / не використовується
Method and system for disaster mitigation planning and business impact assessment – Метод і система формування планів реагування на КС та оцінки впливів на бізнес [31] (США)	Сценарії КС, параметри технічного, фінансового характеру щодо управління підприємством та планів УББ	Моделювання ситуацій, режиму функціонування ІС чи підприємства в цілому. Експертні підходи	Обчислення фізичних і інших ефектів від КС в грошовому виразі, підбір оптимального набору заходів реагування на КС	Аналіз впливу на бізнес (ВІА), менеджмент / частково використовується

Таблиця 2

Основні ознаки систем управління кризовими ситуаціями

Засіб	Функціонування в нечіткому слабоформалізованому	Застосування в менеджменті ІБ	Підтримка прогнозування КС	Підтримка ідентифікації КС	Підтримка оцінки КС	Підтримка реагування на КС та ліквідації їх наслідків	Універсальність	Використання параметрів, характерних для КС в ІБ
Система раннього виявлення надзвичайних ситуацій [11] (Україна)	-	-	+	+	+/-	+/-	-	-
Система раннього виявлення надзвичайних ситуацій [8] (Україна)	-/+	-	+	+	-	-	-	-
Інтегрована інформаційно-аналітична система моніторингу та моделювання антикризового розвитку підприємства [12] (Україна)	-	+/-	-/+	-/+	+	+	+	-
Спосіб прогнозування викиднебезпечності масиву гірських порід [13] (Україна)	-	-	+	+	-	-	-	-
Спосіб прогнозування аварійних ситуацій в підземних гірничих виробках [2, 14] (Україна)	-	-	+	-	-	-	-	-
Програмний страт моделі управління кризовими ситуаціями [16] (РФ)	-	-/+	+	-/+	-/+	-	-/+	-
Автоматизована система підтримки дій диспетчера небезпечного виробництва при виникненні аварійних ситуацій [20] (РФ)	-	-	+/-	+/-	+	+	-/+	-
Система для зменшення збитків та руйнувань в результаті стихійних лих [21] (США)	-	-	+	-	-	+	-	-
System for reducing disaster damage [22] (США)	-	-	+	+/-	+/-	-	-	-
Statistical-determ. approach to natural disaster prediction [24] (США)	-	-	+	+	-	-	-	-

Method and apparatus for disaster prevention [25] (США)	-	-	-	+	-	+	-	-
Dynamic emergency disaster plan [26] (США)	-	-	-	+	-	+	-	-
Method and apparatus for quantifying an impact of a disaster on a network [28] (США)	-	+	+/-	-/+	+	-/+	+/-	-/+
System, method and program for estimating risk of disaster in infrastructure [29] (США)	-	+	+	-	+	-	-	-
Disaster prediction system [30] (США)	-	-	+	+	-	-	-/+	-
Method and system for disaster mitigation planning and business impact assessment [31] (США)	-	+/-	-	-	+	+	-/+	-

У таблиці використані такі позначення: + – так, +/- – частково, скоріше так, -/+ – скоріше ні, - – ні. Під універсальністю розуміється характеристика, що визначає здатність системи бути використаною для управління КС різного роду та походження в різних галузях без необхідності їх пере налаштування з підтримкою більшості ключових етапів КУББ.

Висновки

Проведений аналіз відомих систем та засобів управління КС, що включає в себе прогнозування, ідентифікацію, оцінку КС та реагування на неї з метою виділення основних принципів їх побудови, переваг та недоліків. Аналіз показав, що значна частина розробок в даній галузі ґрунтується на застосування різноманітних датчиків та порогового механізму за принципом компаратора. Недоліком таких систем є складність їх застосування в умовах невизначеності та виникненні невідомих типів КС. Також відомі системи, що під час своєї роботи застосовують історичні, статистичні та математичні методи (статистичні закони розподілу, теорія ймовірностей, Байєсівські мережі тощо), які є надто ресурсоемні та трудомісткі. Також відсутні універсальні системи, що можуть бути застосовані в будь-якій галузі та на всіх етапах управління КС. Крім того практично повністю відсутні системи, що можуть використовуватися в менеджменті ІБ та функціонувати в умовах невизначеності. Жодна з проаналізованих систем не оперує параметрами, характерними для КС в ІБ. Таким чином застосування методів нечіткої логіки та експертних підходів дасть змогу ефективно функціонувати системам управління КС, розробленим на їх основі, в умовах слабоформалізованого простору, а також зменшить ресурсоемність таких технологій за рахунок відсутності потреби збирання та обробки статистичних даних, проведення громіздких та складних математичних обчислень тощо.

Література

[1] Деклараційний патент на винахід 60237 А Україна, МПК G05D 16/00, G05D 27/00. Спосіб автоматичного керування в аварійній ситуації на газопроводі / А. Я. Кацєруба (UA); Ю. Г. Мокеєв (UA); О. Ф. Немчин (UA); Ф. О. Павленко (UA); В. П. Рогатін (UA); В. С. Тарашевський (UA); В. Г. Чернишов (UA). – № 2003054939; заявл. 29.05.2003; опубл. 15.09.2003, Бюл. № 9. – 3 с.

[2] Деклараційний патент на корисну модель 45451 Україна, МПК E21F 5/00, E21C 39/00. Спосіб прогнозування аварійних ситуацій в підземних

гірничих виробках / В. І. Муравейник (UA); С. О. Алексєєнко (UA); Ю. Ф. Булгаков (UA); В. І. Король (UA); І. А. Шайхлісламова (UA). – № u200905789; заявл. 05.06.2009; опубл. 10.11.2009, Бюл. № 21. – 5 с.

[3] Деклараційний патент на винахід 65121 А Україна, МПК E21F 17/18 (2007.01), G08B 31/00. Автоматизована система протиаварійного захисту шахти / В. Г. Курносєв (UA); В. В. Сієнєко (UA); Я. Л. Красієк (UA); П. Я. Большаков (UA); Г. В. Курносєв (UA); Є. Д. Дубов (UA); П. Є. Мухін (UA); В. М. Сірєнєко (UA); О. А. Сіроткін (UA). – № 2003065179; заявл. 05.06.2003; опубл. 15.03.2004, Бюл. № 3. – 4 с.

[4] Деклараційний патент на винахід 67490 А Україна, МПК E21C 35/24 (2007.01). Спосіб протиаварійного захисту шахти / В. Г. Курносєв (UA); В. В. Сієнєко (UA); Г. В. Курносєв (UA); В. М. Сірєнєко (UA); О. А. Сіроткін (UA); Я. Л. Красієк (UA); П. Я. Большаков (UA); Є. Д. Дубов (UA); П. Є. Мухін (UA). – № 2003109045; заявл. 06.10.2003; опубл. 15.06.2004, Бюл. № 6. – 2 с.

[5] Патент 20114 А Україна, МПК G06Q 10/00. Спосіб збору, аналізу інформації, прийняття рішень та оповіщення про виникнення позаштатної ситуації і пристрій для його здійснення / О. В. Грецов (UA). – № 94117818; заявл. 30.11.1994; опубл. 25.12.1997, Бюл. № 6. – 7 с.

[6] Деклараційний патент на винахід 45896 А Україна, МПК G08B 25/00. Спеціальна система індивідуального оповіщення про надзвичайні (небезпечні) ситуації / О. Л. Радєнєко (UA). – № 2001106880; заявл. 10.10.2001; опубл. 15.04.2002, Бюл. № 4. – 2 с.

[7] Деклараційний патент на корисну модель 41967 Україна, МПК G06F 11/00. Комп'ютерна система моніторингу і визначення місця аварії силових мереж сцб / Б. С. Стогній (UA); М. Ф. Сопель (UA); О. І. Стасюєк (UA); В. Л. Тутик (UA); І. О. Щєрбаєкова (UA); А. Л. Жєлєзняєк (UA); Л. Л. Гончарова (UA); Є. Г. Подлєсних (UA). – № u20080819; заявл. 17.06.2008; опубл. 25.06.2009, Бюл. № 12. – 12 с.

[8] Деклараційний патент на корисну модель 32834 Україна, МПК G08B 19/00. Система раннього виявлення надзвичайних ситуацій / Л. П. Пашкєвич (UA). – № u200805031; заявл. 04.03.2010; опубл. 12.04.2010, Бюл. № 7. – 3 с.

[9] Деклараційний патент на корисну модель 49115 Україна, МПК G08C 19/00, G08B 19/00, G08B 21/00. Система раннього виявлення надзвичайних ситуацій (СРВНС) / А. П. Йора (UA); С. М. Сидоров (UA). – № u201002449; заявл. 04.03.2010; опубл. 26.04.2010, Бюл. № 8. – 4 с.

[10] Декларацийний патент на корисну модель 53753 Україна, МПК G08B 19/00. Система раннього виявлення надзвичайних ситуацій / В. І. Ліпчанський (UA); І. В. Плотников (UA); Д. В. Плотников (UA). – № u201009986; заявл. 12.08.2010; опубл. 11.10.2010, Бюл. № 19. – 4 с.

[11] Пат. на корисну модель 79381 Україна, МПК G08B 19/00, G08B 21/00, G01W 1/02, G08C 17/00. Система раннього виявлення надзвичайних ситуацій / Г. О. Федосов, О. О. Юр'єв, В. В. Магда, А. В. Леденьов, С. А. Матвієнков, С. М. Сидоров, О. В. Меркулов (UA). – № u201220210; опубл. 25.04.2013, Бюл. № 8. – 5 с.

[12] Пат. на корисну модель 49154 Україна, МПК G06Q 10/00. Інтегрована інформаційно-аналітична система моніторингу та моделювання антикризового розвитку підприємства / В. А. Корестильов (UA). – № 200909074; заявл. 02.09.2009; опубл. 26.04.2010, Бюл. № 8. – 5 с.

[13] Патент № 47889 Україна, МПК (2006) E21F5/00, E21C 39/00. Спосіб прогнозування виклику небезпечності масиву гірських порід / В. І. Гаркушенко та ін. (Україна). – № 2001107074; Заявл. 18.10.2001; опубл. 15.07.2002, Бюл. № 8. – 6 с.

[14] Муравейник В. И. Теоретические основы и практика оперативного прогнозирования аварийных ситуаций в шахтах / В.И. Муравейник, С.А. Алексеенко, Ю.Ф. Булгаков, И.А. Шайхлисламова, В.И. Король // Науковий вісник НГУ. – 2009. – № 9. – С. 46-50.

[15] Гуляев Э.А. Влияние обратных полярностей в нашей жизни / Э.А. Гуляев, Ф.И. Гуляева. – Одесса: Optimum, 2008. – 7 с.

[16] Суханов Д. В. Программный страт модели управления кризисными ситуациями. / Д. В. Суханов // Вестник СГУТиКД. – 2012. – № 2 (20) . – С. 106-110

[17] Комплекс автоматизированных систем раннего выявления чрезвычайных ситуаций и оповещения ОАО "Запорожжкокс" / Е.А. Соловьев, Л.Я. Эйдельштейн, А.Н. Севастьянов, С.С. Кацило, Ю.А. Чернышов // Матеріали 11-ї Всеукраїнської наук.-практ. конф. «Організація управління в надзвичайних ситуаціях». К.: ІДУЦЗУ УЦЗУ, 2009. – 425 с.

[18] Кузьмин С.П. Автоматизированная система централизованного оповещения категорированного города с численностью населения от 250 до 300 тысяч человек [Текст] / С.П. Кузьмин // Вестник Самарского отраслевого научно-исследовательского института радио, 2009. – С. 65-67.

[19] Актуальные проблемы гражданской защиты. Материалы одиннадцатой Международной научно-практической конференции по проблемам защиты населения и территорий от чрезвычайных ситуаций. 18-20 апреля 2009 г. / МЧС России. – Н. Новгород: Вектор-ТиС, 2009. – 386 с.

[20] Метод прогнозирования последствий и модель автоматизированной системы поддержки принятия решений диспетчера опасного производства при возникновении аварийных ситуаций / В. А. Лыфарь, С.А. Вамболь, Т. В. Гайденок, М. Л. Угрюмов // Открытые информационные и

компьютерные интегрированные технологии. – 2011. – № 51. – С. 178-185.

[21] Patent US006266579B1 USA, Int. Cl. G01M 1/38. System for reducing disaster damage / Mohammad Reza Baraty (USA). – № 09/022,667; declared 12.02.1998; published 24.07.2001. – 18 p.

[22] Patent US007035765B2 USA, Int. Cl. G06F 11/30. Disaster predicting method, disaster predicting apparatus, disaster predicting program, and computer-readable recording medium recorded with disaster predicting program / Shuichi Tanahashi (JP). – № 10/341,479; declared 14.01.2003; published 25.04.2006. – 13 p.

[23] Patent US007932823B2 USA, Int. Cl. G08B 21/00. Disaster noticing system, disaster noticing server, disaster reporting terminal method, and program / Ryosuke Komiya (JP); Hiroaki Kuba (JP); Naoki Kuwamori (JP). – № 12/183,012; declared 30.07.2008; published 26.04.2011. – 25 p.

[24] Patent US007734245B2 USA, Int. Cl. G01V3/00, G01V 7/00, G06G 7/48, G09B 9/56, G01S13/00. Statistical-deterministic approach to natural disaster prediction / Sai Ravela (USA); Kerry A. Emanuel (USA). – № 11/388,185; declared 23.05.2006; published 08.06.2010. – 30 p.

[25] Patent US007436294B2 USA, Int. Cl. G08B 29/00. Method and apparatus for disaster prevention / Susumu Saga (JP); Yasuyuki Kawaida (JP); Hiroko Kaneko (JP). – № 11/193,454; declared 04.08.2005; published 14.10.2008. – 11 p.

[26] Patent US20110299666A1 USA, Int. Cl. H04M11/04. Dynamic emergency disaster plan / Christopher R. Hulls (USA). – № 13/214,181; declared 20.08.2011; published 08.12.2011. – 8 p.

[27] Patent US 20060079200A1 USA, Int. Cl. H04M 11/04. Disaster system control method and disaster system control apparatus / Kiyoshi Hirouchi (JP); Yayoi Itoh (JP); Naoyuki Kakizaki (JP); Saiki Kawamura (JP); Satoru Abe (JP); Yoshikazu Takeda (JP); Takahito Suzuki (JP); Hiroki Yokoyama (JP). – № 11/289,744; declared 29.11.2005; published 13.04.2006. – 46 p.

[28] Patent US007603259B2 USA, Int. Cl. G06F 7/60. Method and apparatus for quantifying an impact of a disaster on a network / Ahmad M. Jrad (US); Blesson Mathews (US); Thomas B. Morawski (US); Louise F. A. Spergel (US). – № 11/238,919; declared 29.09.2005; published 13.10.2009. – 24 p.

[29] Patent US 2006011927A1 USA, Int. Cl. G06Q 99/00, G07G, 1/00, G06F 17/30. System, method and program for estimating risk of disaster in infrastructure / Etienne de Sereville (FR). – № 11/272,299; declared 10.11.2005; published 25.05.2006. – 11 p.

[30] Patent US 20070033153A1 USA, Int. Cl. G06F 15/18. Disaster prediction system / Ryutaro Yamanaka (JP); Hiroyuki Motozuka (JP); Mitsuru Uesugi (JP). – № 10/577,473; declared 25.10.2004; published 07.02.2007. – 35 p.

[31] Patent US20080172262A1 USA, Int. Cl. G06Q 10/00. Method and system for disaster mitigation planning and business impact assessment / Lianjun An (US); Stephen John Buckley (US); Ching-Hua Chen-Ritzo (US); Pawan Raghunath Chowdhary (US); Thomas

Robert Ervolina (US); Daniel A. Ford (US); Igor Frolow (US); Naveen Lamba (US); Young Min Lee (US); Prakaah Mukkarmala (US); Dharmashankar Subramanian

(US). – № 11/622,705; declared 12.01.2007; published 17.07.2008. – 13 p.

УДК 004.056.53:004.492.3 (045)

Гизун А.И., Корченко А.А., Скворцов С.А. Анализ современных систем управления кризисными ситуациями

Аннотация. Концепция управления непрерывностью бизнеса как перспективное направление оперативного и стратегического менеджмента определяет важность защиты информационных ресурсов в условиях кризисных ситуаций. Так, понятие управление кризисными ситуациями включает в себя их прогнозирование, идентификацию, реагирование на негативные влияния и ликвидация последствий, оценку критичности ситуации, а также процессы поддержки принятия решений и деятельности персонала или функционирование систем. В этой статье проведен анализ современных систем управления кризисными ситуациями, основных методов и методик, на которых они основаны. Целью анализа есть определение перспективных направлений развития науки и техники в данной сфере, выделение основных недостатков в существующих системах. Исследование охватывает как отечественные так и зарубежные разработки. Основное внимание уделено системам прогнозирования появления кризисных ситуаций, поддержки принятия решений и деятельности организаций в условиях неопределенности в слабоформализованном пространстве. Результаты этого исследования могут быть использованы при выборе направлений дальнейших исследований относительно разработки систем выявления и оценки кризисных ситуаций, а также подтверждают целесообразность и обоснованность использования экспертных подходов и методов нечеткой логики.

Ключевые слова: кризисная ситуация, управление, система, метод, разработки, выявление, модель, компьютерная программа, прогнозирование, ликвидация последствий, эвакуация, системы поддержки.

Gizun A., Korchenko A., Skvortsov S. Analysis of modern crisis management systems

Abstract. Concept of business continuity management is the prospective direction of operative and strategy management and it defines the importance of information resources security when crisis influences. Crisis management consists of its forecasting, identification, responding and emergency procedures, crisis assessment and also processes of decision support and personnel activity or systems operation. In this paper the analysis of modern crisis management systems and basic methods was carried out. The main aim of this analysis is defining of science and technique prospective directions and also disadvantages identification in existed systems. This study covers both domestic and foreign developments. The main attention is paid to crisis forecasting systems, decision support and personnel activity systems in uncertainty and weak formalized space. This study results can be used to choose future researches directions for crisis detection and assessment systems and it confirms the feasibility and validity for expert approaches and fuzzy logic methods using.

Key words: crisis, management, system, method, developments, detection, model, software, forecast, emergency procedures, evacuation, support systems.

Отримано 24 лютого 2015 року, затверджено редколегією 11 березня 2015 року
