V. V. Vyshnivskyi, S. V. Prishchepa, D. V. Lande

RANKING OF EVENT WEB-SITES

The article describes the methodology of automatic detection of the event basis of information operations, reflected in thematic information flows. The implementation of this methodology allows you to determine the time frame of the information operation, identify the main events that accompany the information operation, and see the techniques of information impact. Information operations in practice are supported by numerous events, processes, actions. It is assumed that a systematic violation of the typical dynamics of some thematic information flows in the open information space may indicate information operations. In the study of information operations, much attention is also paid to the analysis of the dynamics of information flows, a typical template of information operations, which allows using available analytical tools, for example, correlation analysis, to identify them. The proposed methodology for identifying the event basis of information operations covers the following stages of the research: the formation of a thematic information flow on the topic under study; investigation of the dynamics of the received flow, identification of signs of an information operation; narrowing the timeframe of the information flow, obtaining a representative sample of documents; the definition of the terminological basis for the description of events within the scope of the subject area under study. Identify sources of information about events (if necessary); cluster analysis, identify the main events that accompany the information operation. It is suggested to use as reference primary centroids of clusters certain support words that express the essence of events. The proposed approach allows simple implementation of clustering within the capabilities of the content monitoring system InfoStream. Clusters formed in this way reflect the main events occurring during information operations, provide an opportunity to identify participants in information confrontations, and methods of informational influence that disclose the technique for their implementation.

Keywords: information operations; information flows; detection of events; cluster analysis; model domain.

УДК 004.8+65.05+681.5

Ю. І. КАТКОВ, канд. техн. наук, доцент,
Державний університет телекомунікацій, Київ

АНАЛІЗ ПРИЧИН КРИТИЧНИХ СИТУАЦІЙ В ІНФОРМАЦІЙНО-ІНТЕЛЕКТУАЛЬНИХ СИСТЕМАХ

Розглянуто логічний ряд понять, пов'язаних із категорією «небезпека», що дозволить ранжувати спектр можливих загроз безпеці функціонування складної організаційно-технічної системи (СОТС) у критичних ситуаціях і сприятиме розробці затребуваних адекватних технологій протидії впливам зовнішнього середовища на інформаційну систему із мінімізацією негативних наслідків і, зрештою, дасть змогу вдосконалювати існуючу систему забезпечення безпеки СОТС. З огляду на згаданий логічний ряд понять з'ясовано причини виникнення критичних ситуацій в інформаційно-інтелектуальних системах і запропоновано класифікацію факторів-стресорів, зумовлюваних виникненням критичних знань, котрі, у свою чергу, призводять до критичного стану СОТС.

Ключові слова: інтелектуальні системи; критичний стан системи; фактор-стресор; невизначеність; ризик; виклик; загроза.

ВСТУП

Сьогодні неможливо уявити ***складну організаційно-технічну систему*** **(СОТС)**, що функціонує без упровадження ***інформаційних систем*** **(ІС).** Наприклад, енергетичні та транспортні системи, телекомунікаційні мережі, PDM-система (система управління даними про виріб), виробничі організації тощо, які належать до складу СОТС, неодмінно включають у себе ІС.

Відомо, що ІС у складі СОТС призначено для отримання, обробки, зберігання, відображення чи реєстрації даних про технічний стан конструкцій, систем, елементів, їхні властивості, особливості функціонування заради забезпечення інформаційних потреб користувачів у разі прийняття рішень стосовно управління технологічними процесами, а також для адаптації елементів СОТС до впливів зовнішнього середовища.

Сучасну ІС можна розглядати як окремий вид організаційно-технічної системи щодо обробки інформації за допомогою технічних і програмних засобів, котра для підвищення якості функціонування СОТС дедалі більше насичується інтелектуальними технологіями на основі штучного інтелекту, з упровадженням до її складу різноманітних ***інтелектуальних систем*** **(ІнтС).**

ІнтС використовуються для генерування варіантів рішень, з яких особа, що приймає рішення, вибирає потрібне. Отже, метою ІнтС є моделювання розумових процесів організації знань, притаманних людині при прийнятті рішень у різних галузях соціально-економічної сфери суспільства на основі засобів і методів штучного інтелекту. Тому сучасні ІС неухильно стають інформаційно-інтелектуальними системами.

Інформаційно-інтелектуальна система **(ІІС)** — це один із видів автоматизованих ІС, що спирається на знання і є комплексом програмних, лінгвістичних і логіко-математичних засобів для реалізації основного завдання: підтримки діяльності людини та пошуку інформації в режимі розширеного діалогу засобами природної мови. Прикладами ІІС є експертні системи, інтерактивні банери, запитально-відповідні системи, інтелектуальні пошукові системи, віртуальні співрозмовники тощо. Вони мають значний рівень упровадження штучного інтелекту на основі хмарних технологій, що спрощує обмін інформацією у вигляді знань у системах людина–людина, людина–пристрій і пристрій–пристрій, як у межах системи, так і при взаємодії із зовнішнім середовищем на базі згаданих знань.

Відомо, що ***знання*** (*knowledge*) — це здобуток процесу пізнавальної діяльності, узагальнений суспільно-історичний досвід, результат опанування дійсності. Поняття «знання» досить розпливчасте. Зазвичай під знанням розуміється добре формалізована інформація або структуровані дані, тобто лише той результат пізнання, який відзначається безумовною істинністю, може бути логічно або фактично обґрунтований і припускає емпіричну чи практичну перевірку. Відомо, що знання — більш складна категорія інформації, аніж дані, бо дані — це інформація фактичного характеру, що описує об'єкти, процеси і явища предметної області, а також їхні властивості. Натомість знання описують не тільки окремі факти, а й взаємозв'язки між ними. Знання в СОТС розглядаємо як досвід щодо типових рішень в однакових ситуаціях. Вочевидь, якщо для прийняття рішення бракує знань, виникає ситуація прояву критичних знань.

Критичні знання (*critical knowledge*) — це знання, за відсутності яких неможливо забезпечити безперебійну роботу деякої СОТС. Практично йдеться про мінімальну кількість інформації, необхідної для прийняття рішень при виконанні певних функцій, особливо важливих для забезпечення успішної роботи тієї чи іншої організації. Опанування критичних знань вважається обов'язковим для досягнення необхідних результатів при виконанні інтелектуальних завдань, пов'язаних із різноманітними виробничими процесами або функціональними обов'язками, які передбачено посадовими інструкціями. Брак таких знань (недостатність інформації для прийняття рішення), коли йдеться про роботу ІІС, унеможливлює прийняття типових рішень за певних умов впливу зовнішнього середовища, що призводить до ***критичного стану СОТС***. Типові рішення, формалізовані внаслідок обробки багатьох даних (інформації) стосовно деякої ситуації, зберігаються в базі знань у вигляді моделей-образів.

Сукупність взаємозв'язаних ІІС являє собою ***інформаційну інфраструктуру СОТС***. Відомо, що інформаційна інфраструктура (*information infrastructure*) — це комплекс програмно-технічних засобів, організаційних систем та нормативних баз, який забезпечує взаємодію інформаційних потоків, функціонування й розвиток засобів інформаційної взаємодії та інформаційного простору СОТС. Упровадження штучного інтелекту у вигляді ІІС у поєднанні з хмарними технологіями збільшує питому вагу розумових функцій при автоматизації процесів управління, підвищуючи ефективність функціонування СОТС.

Природно, що в умовах інформатизації суспільства з елементами інтелектуалізації окремих процесів на основі штучного інтелекту виникає ймовірність завдання шкоди (зниження ефективності функціонування СОТС) різної тяжкості комусь або чомусь у складі СОТС, що зумовлюється наявністю певних об'єктивних і суб'єктивних зовнішніх чинників, котрі мають вплив на безпеку функціонування СОТС. Тому розуміння сутності концепту безпеки функціонування СОТС за умов впливу зовнішнього середовища на ІІС нерозривно пов'язане з категорією «небезпека».

Небезпека — це негативний вплив (шкода, збиток, шкідливий вплив, ураження), тобто все те, що призводить до зниження ефективності функціонування СОТС. Небезпека розглядається як сукупність факторів, що негативно впливають на природу, людину, суспільство, технічні системи, і характеризуються гіпотетичністю, відсутністю адресності. Вона формується зовнішнім середовищем і може відвертатися або нейтралізуватися шляхом запобігання критичним ситуаціям. Відомо, що небезпека під дією зовнішнього середовища може мати різні рівні прояву негативного впливу стосовно уразливого об'єкта. Тому є сенс побудувати згадуваний уже логічний ряд понять, які відображають різні рівні прояву небезпеки щодо адресного уразливого об'єкта: «невизначеність», «ризик», «виклик», «загроза».

Відмінності між даними поняттями можна визначити за допомогою співвідношення суб'єктивних намірів і об'єктивних можливостей об'єктів та суб'єктів безпеки. Натомість спільною для них усіх рисою є ступінь небезпеки заподіяння шкоди або ураження об'єктам СОТС, у тому числі для інформаційної інфраструктури.

Метою цієї статті є визначення основних факторів-стресорів, які впливають на виникнення критичних знань, що призводять до критичного стану ІІС.

Об'єктом дослідження у пропонованій статті є ІІС, що належать до класу автоматизованих систем із розумовими функціями для керування СОТС. ***Предметом дослідження*** є основні

фактори-стресори, які впливають на виникнення критичних знань.

Таким чином, актуальність вибраної теми не викликає сумніву. Адже за умов упровадження ІІС у сучасні СОТС необхідно розгортати дослідження щодо умов виникнення кризових ситуацій функціонування та способів запобігання їм.

Постановка завдання

Розглядається СОТС, в якій є множина ІІС, розташованих у ієрархічній структурі системи управління. Інтелектуальні складові об'єднано в деяку ІІС, на яку можуть діяти різні рівні небезпеки. Їхній вплив призводить до появи критичного стану або в елементах інтелектуальної системи, або в елементах інформаційної системи, або в усім СОТС. Потрібно визначити сукупність факторів-стресорів для подальшої їх формалізації та побудови моделей захисту.

Аналіз останніх досліджень і публікацій

В [1] показано, що в СОТС завжди існує критичний елемент, вплив на який з боку небезпеки може призвести до критичного стану всю систему. У [2] висвітлено роль і місце інформаційної інфраструктури під час виникнення явища критичності в СОТС. У [3] розглянуто критичні технології та їхній вплив на систему. Але розгляд причини виникнення критичності знань в ІІС та умов появи небезпек різних рівнів для ІІС виконується вперше, що є актуальним завданням.

ОСНОВНА ЧАСТИНА

Виходимо надалі з того, що побудова згадуваного вже логічного ряду понять, пов'язаних із категорією «небезпека», що відображають різні рівні прояву небезпеки, дозволить ранжувати спектр можливих загроз безпеці функціонування СОТС, а також сприятиме розробці актуальних і адекватних технологій протидії впливам зовнішнього середовища, мінімізації негативних наслідків і, отже, дозволить вдосконалити існуючу систему забезпечення безпеки СОТС.

Невизначеність — це мінімальна небезпека, яку, з одного боку, слід розглядати як вияв неоднозначності тенденцій зміни стану об'єкта з плином часу внаслідок негативної дії зовнішнього середовища, а з другого боку, невизначеність є джерелом ризику, який визначає ймовірність завдати шкоди об'єкту безпеки, що перебуває в стані динамічної рівноваги та постійно змінюється. Це провісник появи ризику зміни об'єкта в часі під негативним впливом зовнішнього середовища. Доцільно оцінювати невизначеність кількістю інформації про тенденції зміни об'єкта в часі внаслідок негативного впливу зовнішнього середовища. Сьогодні відомі такі методи оцінювання інформації: обсяговий (кількість символів у повідомленні), ентропійний (на основі статистичної кількісної міри відповідно до теореми К. Шеннона), алгоритмічний (семантичний, структурний).

Ризик — це виявлена негативна тенденція розвитку системи, що знижує (або ускладнює) можливості існування і позитивного розвитку системи. Це небезпека, яка поєднує ймовірність та наслідки настання несприятливих подій, а точніше — рівень небезпеки, який можна визначити ймовірністю настання несприятливої події. Знання ймовірності несприятливої події дозволяє визначити ймовірність сприятливих подій за формулою $P\{+\} = 1 - P\{-\}$. Ризиком часто називають також певну подію, здатну завдати шкоди (збиток, негативний вплив, ураження) комусь або чомусь.

Виклик — виявлення (прогнозування ймовірності появи) можливих негативних впливів зовнішнього середовища на стан елементів СОТС, довільний розвиток яких неминуче призведе до погіршення загального стану цієї системи із загрозою самому її існуванню. Виклики мають загальний природно-соціальний характер (зміна умов функціонування, катастрофічна екологія і демографія, дефіцит ресурсів або сировини тощо), являючи собою мінімальний ризик. Виклик вирізняється потенційною здатністю завдати шкоди СОТС.

Оцінювати виклик доцільно ймовірністю формування негативних впливів зовнішнього середовища на стан конкретних елементів СОТС.

Загроза (*threat*) — це максимальна небезпека (будь-які потенційні чи реальні обставини або події), що виникає в зовнішньому середовищі і може спричинити порушення існуючого стану функціонування конкретних елементів СОТС, скажімо через недодержання технології управління, політики безпеки інформації чи завдання збитків автоматизованій системі. Це стадія крайнього загострення суперечностей, стан, що передує реальному конфлікту. Отже, загроза являє собою найбільш конкретну й безпосередню форму небезпеки або сукупність умов і факторів, що ставлять під удар досягнення цілей СОТС. Загроза характеризується реальністю, адресністю, високим ступенем готовності щодо завдання шкоди об'єкту безпеки. Загрози — це небезпеки, що реалізуються. Загроза може бути передумовою порушення одного чи кількох аспектів безпеки, неприпустимого ризику в разі прийняття керуючих рішень. Існують природні та штучні, навмисні та випадкові загрози. Спробу реалізації загрози називають ***атакою***. Оцінювати загрозу прийнято ймовірністю ураження конкретних елементів СОТС.

Згадуваний раніше логічний ряд понять, що стосуються категорії «небезпека» для ІІС, ранжує ймовірність завдання ІІС шкоди різної тяжкості, зумовленої наявністю певних об'єктивних

і суб'єктивних чинників. Отже, ідеться про реальну можливість негативного впливу, здатного погіршити стан уразливого об'єкта, коли всі рівні небезпеки стосуються деяких уразливих елементів ІІС.

Уразливий об'єкт — це слабка ланка в організаційній системі, наявність якої призводить до нездатності зазначеного об'єкта протистояти шкідливим впливам (небезпекам, загрозам), дія яких порушує технологію управління. Якщо цей об'єкт відіграє важливу роль у системі, то його пошкодження (втрата) може спричинити катастрофічні наслідки.

Розрізняють людську, технічну та інформаційну уразливість. Перша виникає внаслідок психологічних впливів. Технічна зумовлюється несправністю засобів управління системою. Інформаційна уразливість є наслідком непередбаченого впливу інформації на процес прийняття рішень. Загроза і уразливий об'єкт є передумовами виникнення критичного стану інфраструктури.

Унаслідок впливу певного виду небезпеки на деякий елемент ІІС маємо ситуацію критичності знань. Тому актуальним є виявлення основних факторів, які впливають на виникнення саме критичних знань, що призводять до критичного стану ІІС. Це змушує уточнити низку понять.

Інтелектуалізація СОТС — збільшення питомої ваги розумових функцій (управління, контроль, налагодження) у структурі трудових зусиль працівника на основі науково-технічного прогресу, підвищення кваліфікаційного та культурно-освітнього рівня трудящих [4].

Інтелектуальні технології **(ІнтТ)** — це сукупність самих лише інформаційних процесів, які використовують засоби та методи, пов'язані з генеруванням, аналізом, інтерпретацією і використанням різноманітних даних щодо розробки варіантів рішень безпосередньо в тій системі, в якій генеруються відповідні дані. Мета ІнтТ — за допомогою методів штучного інтелекту зменшувати затримки, витрати і ризики безпеки інформаційної технології в певній галузі виробництва, а також забезпечувати науковий опис способів виробництва, тим самим підвищуючи ефективність функціонування різноманітних систем. ІнтТ є окремим видом ІТ. Нині умовно визначають такі категорії ІнтТ: *експлуатаційні* (забезпечення функціонування всіх житлово-експлуатаційних служб мікрорайону), *інтернету речей* (контроль, управління і обробка інформації від «речей», оснащених сенсорами, датчиками і пристроями передавання інформації) та *керування складними системами* (інформаційно-пошукові інтернет-системи, робототехніка, енергетичні та транспортні системи, телекомунікаційні мережі, виробництво і т. ін.). На основі ІнтТ створюються ІІС.

Зауважимо, що протягом багатьох років різні експерти робили спроби сформулювати універсальне визначення ***інтелектуальної системи***. У результаті з'явилося безліч визначень, в яких «інтелект» системи нерідко розглядається з кардинально різних позицій. Проте в жодному з визначень не піддається сумніву, що, по-перше, така система функціонує без участі людини; по-друге, ключовим елементом зазначеної системи є сучасна мережна інфраструктура, що забезпечує під'єднання і взаємодію різних систем; по-третє, вона генерує знання та моделює розумові процеси, притаманні людині при прийнятті рішень; по-четверте, необхідною частиною будь-якої інтелектуальної системи є знання; по-п'яте, вона є складовою ІС.

Унаслідок того, що існують категорії інтелектуальних технологій (експлуатаційні, інтернету речей та керування складними системами), одні автори вважають, що ІІС включає в себе персонал, який її експлуатує, а інші заперечують це. Тому ІІС за ступенем автоматизації поділяють на два класи: ***автоматизовані***, що припускають участь людини (інтелектуальні системи для керування складними системами), та ***автоматичні***, без її участі — різні ро́боти (експлуатаційні інтелектуальні системи або інтелектуальні системи інтернету речей). Прикладом автоматизованих ІІС є пошукові бібліотечні інформаційні системи, в яких користувач із множини джерел знаходить одне потрібне йому. До автоматичних належать деякі пошукові інтернет системи, такі як Google, де збір інформації по сайтах здійснюється пошуковим роботом (grabber, «Web spider», crawler) і людський фактор не впливає на ранжування результатів пошуку. Варто зазначити, що межа між автоматизованими та автоматичними ІІС досить умовна і залежить від рівня впровадження в них методів штучного інтелекту, тому й досі термін «інтелектуальні системи» може стосуватись як автоматизованих, так і автоматичних ІІС.

Розглядаючи ІІС, говорять про такі види забезпечення: технічне, інформаційне, програмне та організаційне.

Інтелектуалізація здійснюється на основі штучного інтелекту шляхом створення інтелектуальних систем. Тому далі пропонується визначення, що є компіляцією багатьох відомих [4–7] .

Інтелектуальна система **(***intelligent systems***, ІнтС)** — це складова ІІС, адаптивна, автоматизована або автоматична. Це програмно-технічна система для генерування знань, які забезпечують розв'язування неформалізованих завдань користувача в певній предметній галузі, знання про яку зберігаються в пам'яті такої системи, та організовує його взаємодію з комп'ютером у звичних поняттях, термінах, образах. Метою ІнтС є генерування

знань та моделювання розумових процесів, притаманних людині при прийнятті рішень у різних галузях соціально-економічної сфери суспільства в умовах різноманітних загроз. ІнтС бувають різного призначення, вони можуть оперувати даними і самонавчатися. Сфери застосування ІнтС необмежені: від створення *інтелектуалізованих систем і засобів* (робототехнічних систем; комп'ютерних інтерфейсів, онлайн-перекладачів у реальному часі, мульти- і гіпермедійних технологій віртуальних середовищ, інтелектуальних сенсорних системи тощо) до *інтелектуальних систем* (моделювання інтелектуальної діяльності людини, експертні інтелектуальні системи, інтелектуально-пошукові системи, інтелектуальні системи прийняття рішення і управління складними системами). У загальнотеоретичному розумінні ІнтС — це синонім терміна «розумна система», яка з точки зору системного підходу може розглядатися як складна система, здатна, з одного боку, сприймати, порівнювати, перетворювати інформацію про події та явища навколишнього середовища за допомогою формалізованих інтелектуальних моделей-образів, а з другого боку, створювати і зберігати в собі моделі-образи певних об'єктів. Модель-образ — це об'єкт, структура якого пов'язана зі структурою об'єкта-прототипу деяким відношенням подібності або подоби. Необхідною частиною будь-якої інтелектуальної системи є знання.

Інтелектуальна загроза — сукупність умов і факторів, що створюють небезпеку раціональному використанню розумової діяльності, зменшують розумові здібності людей, спотворюють (нав'язують) їм хибні рішення в разі їхньої управлінської діяльності. У процесі управління складними системами досить часто виникають різні, у тому числі непередбачувані критичні або позаштатні ситуації. Приклади таких ситуацій: загроза поразки внаслідок зовнішніх причин, загроза зіткнення, загроза виявлення, відмова або нештатна робота обладнання, критична нестача енергії для виконання наміченої програми досліджень, неконтрольоване поводження складної системи.

Уразливість в інформаційній системі є подією, за якої компрометується один або кілька аспектів безпеки інформації (доступність, конфіденційність, цілісність і достовірність). Наявність уразливого об'єкта створює слабку ланку, що може призвести до порушення безпеки інформації. Природно, що вплив загрози на технологію управління може викликати критичний стан будь-якої організаційної системи — як її складових, так і всієї системи. Звідси правомірно передбачати залежність безпеки будь-якої СОТС від рівня інформаційної безпеки ІІС.

Критичний стан об'єкта — це поняття, що стосується організаційної системи. Воно в загальному випадку характеризує реакцію об'єкта на дію зовнішнього середовища, коли цей об'єкт раптово втрачає свої задані властивості внаслідок дії середовища і набуває інших, які не могли бути передбачені на етапі проектування об'єкта.

Для запобігання кризовому стану в організаційній системі виконуються заходи з її реформування із застосуванням методів цільового управління та відповідних технологій управління, як це показано в [2]. Під критичним станом інтелектуальної системи будемо розуміти ситуацію, мала зміна якої може якісно змінити стан або процес у цілому («ефект метелика»).

Під ***критичними ситуаціями інтелектуальних систем*** будемо розуміти ситуації, мала зміна яких може якісно змінити стан системи (ІнтС, ІІС, СОТС), процесу або проблеми в цілому. Наприклад, поширення вірусів через інтернет-канали призводить до ураження обладнання ІІС, використовуваного для зберігання та обробки високовартісних баз даних, а внаслідок зміни цих даних можуть генеруватися хибні рішення, що призведуть до лавиноподібних економічних збитків. Отже, необхідно протидіяти цим загрозам шляхом організації захисту уразливих об'єктів ІІС.

Криза організаційної структури — це переломний момент, небезпечне нестійке положення, перехідний стан, за якого існуюча організаційна структура для вирішення завдань уже неадекватна цим завданням, у результаті чого виникають непередбачувані кризові ситуації. Традиційними ознаками кризи є порушення відповідності між попитом і пропозицією, між потребами і забезпеченням. Природа кризи приховується в наявності уразливого об'єкта відносно певної загрози.

Система з критичною інфраструктурою (критична система) — це сукупність фізичних або віртуальних систем і засобів, настільки важливих для держави, що їх вихід із ладу або знищення може призвести до згубних наслідків у галузі оборони, економіки, охорони здоров'я і безпеки нації [4]. Зазначене поняття охоплює ключові галузі, де є уразливі об'єкти: органи управління; інформаційні і телекомунікаційні системи та мережі; енергетику; транспорт; фінансові системи тощо. Стан цих галузей має вплив на рівень воєнної, економічної, екологічної та інших видів безпеки.

Аналіз причин критичних ситуацій в ІІС

Основними стримуючими факторами в розробці ІІС є невирішені проблеми розпізнання критичного стану в СОТС. У медицині, фізіології, психології є поняття «стрес» та різні його види, наприклад нервово-психічний, температурний, світловий тощо. ***Стрес*** (*stress*) — навантаження,

напруга; стан підвищеної напруги. Ідеться про сукупність неспецифічних адаптаційних (нормальних) реакцій системи (організму) на вплив різних несприятливих факторів-стресорів, що порушує його гомеостаз, а саме: саморегуляцію, здатність відкритої системи зберігати сталість свого внутрішнього стану за допомогою скоординованих реакцій, спрямованих на підтримку динамічної рівноваги.

Упровадження технологій на основі штучного інтелекту дозволяє використати наукові результати, здобуті в згаданих галузях. Скажімо, поняття «стрес» щодо соціально-біологічної системи є сенс вважати тотожним поняттю «криза» для СОТС, що характеризує особливості виникнення критичного стану елементів ІІС у сфері інтерпретації знань, адекватного зберігання та обробки тривимірної візуальної інформації.

Як причини виникнення таких кризових ситуацій СОТС слід розглядати різноманітні ***фактори-стресори***, пов'язані з критичними знаннями. На них можуть впливати соціальні та ситуаційні фактори; індивідуальні та біологічні особливості самої людини; характер та інтенсивність факторів впливу, що викликають стресову ситуацію.

Фактори-стресори можуть бути або гострими (раптово виникають), небезпечними (природні та техногенні катастрофи, аварії), або хронічними, постійними, розтягнутими в часі (соціально-економічні труднощі, конфліктні ситуації тощо). Фактори-стресори поділяються на поодинокі, множинні та періодичні. Фактори-стресори, що призводять до кризи, подібні матрьошці: накопичуються один за одним. Але слід підкреслити, що криза — це не безвихідь, а деякі суперечності, через які проходить система на шляху свого становлення. Знаючи природу факторів-стресорів, тобто природу виниклої суперечності, можна вибирати необхідні засоби протидії для досягнення поставлених системі цілей.

На основі визначеного понятійного апарату можна виконати ***класифікацію факторів-стресорів***, які призводять до появи критичних знань, що, у свою чергу, спричинюють критичний стан ІІС.

Пропонована класифікація включає в себе п'ять класів.

1. Спеціальні (умисні) спотворення повноти здобутих знань. Для того щоб наділити систему знаннями, їх необхідно здобути. У процесі здобуття знань формуються: декларативні та процедурні знання. ***Декларативні знання*** описують факти і явища, фіксують наявність або відсутність таких фактів, а також включають у себе описи основних зв'язків і закономірностей, до яких ці факти і явища причетні. ***Процедурні знання*** описують дії, можливі при маніпулюванні фактами і явищами для досягнення намічених цілей. Факт у широкому сенсі може виступати як синонім істини; подія або результат; реальне, а не вигадане; конкретне і поодиноке на противагу загальному і абстрактному. Факти вказують на добре відомі в даній галузі обставини. З них народжується ***евристика***. Евристика спирається на власний досвід експерта, який працює в конкретній предметній галузі, накопичений у результаті багаторічної практики. Отже, *критичним моментом у знаннях є спотворення повноти здобутих знань*.

2. Спеціальні (навмисні) спотворення форми подання знань. Для того щоб наділити систему знаннями, їх необхідно подати в певній формі. Існують два основні способи наділити знаннями програмну систему: помістити знання в програму та подати їх у певному форматі, умістивши в базу знань. Звідси можна достатньо впевнено стверджувати, що при розміщенні знань у програмі можуть бути внесені або хибні знання, або знання з двояким (неправильним) змістом, або знання, що не відповідають фактичним умовам (застарілі дані). Що ж до бази знань, які є моделями людських знань (зафіксованих в енциклопедіях і довідниках), то весь обсяг знань, які є в людей, залучених до процесу вирішення складних завдань, змоделювати неможливо хоча б через брак часу. Отже, *критичним моментом у знаннях є можливість спотворення форми подання знань*.

3. Порушення правильних взаємозв'язків або створення завідомо неправдивих взаємозв'язків між даними. Необхідною частиною будь-якої інтелектуальної системи є знання. Відомо, що знання є більш складною категорією інформації порівняно з даними. Адже дані — це інформація фактичного характеру, що описує об'єкти, процеси і явища предметної області, а також їхні властивості, а знання описують не тільки окремі факти, а й взаємозв'язки між ними. Отже, *критичним моментом у знаннях є порушення справжніх взаємозв'язків або створення завідомо неправдивих взаємозв'язків між даними*.

4. Втрата корпоративної пам'яті (рівня компетенції в організації). Підтримка корпоративної пам'яті (сумарних знань усіх людей, що працюють в організації чи відомстві) або рівня компетенції в організації стає однією із серйозних проблем. Ідеться про те, що з часом багато фахівців (експертів), які є носіями виробничого досвіду або ексклюзивних евристичних знань у тій чи іншій галузі виробництва, можуть залишати цю організацію. Природно, що при цьому вони винесуть із собою значну кількість практично необхідних знань і корпоративної пам'яті, потрібних для безперервного і надійного функціонування будь-якої складної системи. Виникає дефіцит кваліфікованих співробітників зі зниженням рівня компе-

тенції в організації. Керівникам організацій слід враховувати цей фактор для розробки стратегічного підходу, який охоплює проблеми, пов'язані з можливістю втрати корпоративної пам'яті. Більш того, кожний керівник повинен постійно давати оцінку ситуації у своїй організації і відповідно до власних специфічних потреб адаптувати або змінювати концепції, методи та засоби управління. Отже, *втрата таких працівників, які володіють знаннями, важливими з погляду як експлуатації, так і безпеки, є очевидною внутрішньою загрозою щодо безпечної і надійної експлуатації обладнання, організації функціонування окремих підрозділів системи*.

5. Неповна і хибна інформація про об'єкт (хибні і неповні дані). Якщо дані відібрані або зібрані неправильно (неточно визначено набір самих параметрів або дані містять помилки), то такі дані не зможуть відобразити істотні властивості стану або поведінки об'єкта управління, потрібні для об'єктивного і достовірного судження про нього та прийняття розумних управлінських рішень. Якщо даних для аналізу бракує, то обсяг здобутої з них необхідної інформації може виявитися також не цілком достатнім для прийняття рішення, а зроблені на таких підставах висновки будуть неповними. Отже, *це позначиться на ефективності управління (слід зазначити, що в теорії інформації та управління розроблено сучасні методи, які дозволяють оптимізувати процеси управління в умовах неповної інформації про об'єкт)*.

ВИСНОВКИ

Запропонований логічний ряд понять, пов'язаних із категорією «небезпека», дозволяє:

♦ ранжувати спектр можливих загроз безпеці функціонування СОТС;

♦ сприяти розробці актуальних і адекватних технологій протидії негативним впливам зовнішнього середовища, із мінімізацією негативних наслідків і подальшим удосконаленням існуючої системи забезпечення безпеки СОТС;

♦ виявляти причини виникнення критичних ситуацій в інтелектуальних системах і класифікувати фактори-стресори, які впливають на виникнення критичних знань, а отже, і критичного стану системи:

1) спеціальні (навмисні) спотворення повноти здобуття знань;

2) спеціальні (навмисні) спотворення форми подання знань;

3) порушення правильних взаємозв'язків або створення завідомо неправдивих взаємозв'язків між даними;

4) втрата корпоративної пам'яті (рівня компетенції в організації);

5) неповна чи хибна інформація про об'єкт (спотворені та неповні дані).

Список використаної літератури

*1. **Вишнівський В. В., Катков Ю. І., Сєрих С. О.** Роль і місце інформаційної інфраструктури під час виникнення явища критичності організаційної системи // Зв'язок. 2017. №5. С. 51–56.*

*2. **Даник Ю. Г., Катков Ю. І., Пічугін М. Ф.** Національна безпека: запобігання критичним ситуаціям: монографія. Житомир: Рута, 2006. 386 с.*

*3. **Величко О. Ф., Затинайко О. І., Скурський П. П.** Критичні технології як національний пріоритет у забезпеченні обороноздатності держави // Наука і оборона. 2011. № 4. С. 23–30.*

*4. **Словник** іншомовних слів / за ред. О. С. Мельничука. 1985. 966 с.*

*5. **Аверкин А. Н., Гаазе-Рапопорт М. Г., Поспелов Д. А.** Толковый словарь по искусственному интеллекту. Москва, 1992. 256 с.*

*6. **Философия:** Энциклопедический словарь / под ред. А. А. Ивина. Москва, 2004. 547 с.*

*7. **Никифоров А. Л.** Новая философская энциклопедия. Москва, 2010.*

Рецензент: доктор техн. наук, **В. В. Онищенко**, Державний університет телекомунікацій, Київ.

Ю. И. Катков

АНАЛИЗ ПРИЧИН КРИТИЧЕСКИХ СИТУАЦИЙ В ИНФОРМАЦИОННО-ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЕ

Рассмотрен логический ряд понятий, связанных с категорией «опасность», который позволит ранжировать спектр возможных угроз безопасности функционирования сложной организационно-технической системы (СОТС) и будет способствовать разработке востребованных адекватных технологий противодействия влияниям внешней среды при минимизации негативных последствий, а в результате даст возможность усовершенствовать существующую систему обеспечения безопасности СОТС. Согласно логическому ряду понятий рассмотрены причины возникновения критических ситуаций в интеллектуальных системах и предложена классификация факторов-стрессоров, обусловливающих возникновение критических знаний, которые, в свою очередь, приводят к критическому состоянию интеллектуальную систему.

Ключевые слова: интеллектуальные системы; критическое состояние системы; фактор-стрессор; неопределенность; риск; вызов; угроза.

Yu. I. Katkov

ANALYSIS OF CAUSES OF CRITICAL SITUATIONS IN INFORMATION-INTELLECTUAL SYSTEMS

The article deals with a logical series of concepts related to the category of «danger», namely: «Uncertainty», «risk», «challenge», «threat». It is shown that the differences between these concepts can be determined with the help of the ratio of subjective intentions and objective capabilities of objects and subjects of security. The common for them all feature is the degree of danger of causing harm or damage to objects. This will allow to rank the range of possible threats to the dangers of functioning of a complex organizational and technical system, and will also contribute to the development of relevant, adequate technologies to counter the environmental impacts, minimize negative consequences, and as a result, will improve the existing system security system. Concerning the logical series of concepts, the causes of emergence of critical situations in intellectual systems are considered, a classification of stressors factors influencing the emergence of critical knowledge is proposed, which leads to a critical state of the intellectual system, namely: deliberate distortion of the completeness of knowledge acquisition, deliberate distortion of the form of representation of knowledge, violation of the correct relationships or the creation of knowingly false relationships between the data, loss of corporate memory (competence level in the organization, incomplete and incorrect information about the object (incorrect and incomplete data.) The analysis of the causes of critical situations in intelligent information systems allowed to determine the nature of the contradiction, it is shown that the stressors that lead to the crisis can accumulate one after another. If you know the nature of the stressors factors, you can choose the necessary means of struggle to achieve your goals in the system.

Keywords: intellectual systems; critical state of system; factor-stressor; uncertainty; risk; challenge; threat.