Науковий вісник НЛТУ України
Scientific Bulletin of UNFU
https://doi.org/10.36930/40330110
Article received 06.02.2023
Article accepted 27.02.2023
УДК 004.81:681.5
Correspondence author: N. K. Lysa lysa.nataly@gmail.com

ISSN 1994-7836 (print)
ISSN 2519-2477 (online)

Л. С. Сікора[1], Н. К. Лиса[1], О. М. Павлюк[1], В. І. Сабат[2], О. Ю. Федевич[1]

[1] *Національний університет "Львівська політехніка", м. Львів, Україна*
[2] *Українська академія друкарства, м. Львів, Україна*

ІНФОРМАЦІЙНІ ТА ЛОГІКО-КОГНІТИВНІ ПІДХОДИ ДО ФОРМУВАННЯ КІБЕРБЕЗПЕКИ ТЕХНОГЕННИХ ІНФРАСТРУКТУР З УРАХУВАННЯМ РІВНЯ РИЗИКІВ

Розглянуто проблему цілеорієнтованого функціонування складних енергоактивних систем в умовах дії комплексу загроз. Атаки на структуру і процеси управління ускладнюють технологічні процеси і можуть спровокувати аварійні ситуації. Модернізація агрегатів складних технологічних процесів згідно з новими вимогами безпеки для розподіленої просторової інфраструктури вимагає використання нових управлінських систем та комп'ютерних й інформаційних мережевих технологій для передачі й опрацювання даних про стан агрегатів і об'єктів. Це відповідно ставить проблему перегляду базових концепцій побудови інформаційно-вимірювальних систем, розроблення програмного й апаратного забезпечення для реалізації процесу цільового управління, створення сенсорів на основі нових методів відбору даних проблемних ситуацій. Розроблено нові підходи до подання, оброблення, відображення даних про стан агрегатів енергоактивних об'єктів та всієї інфраструктури. При цьому враховано, що як технологічні системи, так і управлінські, мають ієрархічну структуру. Для управління в умовах загроз потрібно врахувати особливості інформаційної інфраструктури, способи відбору й опрацювання даних, методи й алгоритми класифікації ситуації. Інформація про ситуацію формується із блоків даних, отриманих від кожного агрегата і технологічного процесу загалом. Для формування й ухвалення та реалізації керівних рішень необхідна інформація про стан системи в поточному часі та відомості про стан системи і його інфраструктуру. Обґрунтовано процедуру цілеорієнтації та вибрано моделі індикаторів розходження реальних траєкторій параметрів режимів функціонування об'єктів від цільового завдання. Відповідно величина інтервалу відхилення траєкторії відносно еталонної визначає ймовірність ризику від дії атаки на підставі рангів допустимих змін станів енергоактивного об'єкта. Обґрунтовано і процедури ухвалення рішень для координації управлінських дій, яка ґрунтується на знаннях про об'єкт та стратегічній цілеорієнтації організації структури. Обґрунтовано вимоги до професіоналізму та рівня інтелектуальної, когнітивної і наукової підготовки персоналу для різних рівнів ієрархії виробництва й управління та ступеня повноважень у прийнятті рішень. Показано, що вся інформація, необхідна для прийняття рішень на управління командою оперативного персоналу, формується з даних різного типу, які сприймаються з мультимедійних щитів від інформаційної системи АСУ-ТП, які перебувають у полі уваги когнітивної системи кожного з них (як інтелектуальних агентів). Відповідно для кожного рівня ієрархії інфраструктури, орієнтованої на стратегічні цілі в динамічному середовищі глобальної інфраструктури, розроблено методи оцінювання ситуації для виявлення збоїв та дії атак, на підставі яких формуються способи протидії залежно від типу загроз.

Ключові слова: кібербезпека; інфраструктура; система; управління; когнітивні моделі; інформаційні технології; стратегії; ризики; цілеорієнтація; енергоактивність; ієрархія.

Вступ / Introduction

Сучасний етап аналізу динаміки і цілей функціонування інфраструктури цілеорієнтованих ієрархічних систем з корпоративними та іншими видами управління показує, що кризові поточні і надзвичайні ситуації виникають унаслідок минулих проєктних помилок. Невизначеність і чіткість цілей, недооцінка ресурсів, вибір нечітких стратегій і основних цілей, за дії когнітивних збоїв в умовах прийняття рішень, недостатня кваліфікація персоналу, неврахування зовнішніх загроз, невміння прогнозувати активні події на великий термін часу.

Інформація про авторів:
Сікора Любомир Степанович, д-р техн. наук, професор, кафедра автоматизованих систем управління.
Email: lssikora@gmail.com; https://orcid.org/0000-0002-7446-1980
Лиса Наталія Корнеліївна, д-р техн. наук, доцент, кафедра автоматизованих систем управління.
Email: lysa.nataly@gmail.com; https://orcid.org/0000-0001-5513-9614
Павлюк Олена Миколаївна, канд. техн. наук, доцент, кафедра автоматизованих систем управління.
Email: olena.m.pavluk@lpnu.ua; https://orcid.org/0000-0003-4561-3874
Сабат Володимир Іванович, канд. техн. наук, доцент,кафедри інформаційних мультимедійних технологій.
Email: v_sabat@ukr.net; https://orcid.org/0000-0001-8130-7837
Федевич Ольга Юріївна, канд. техн. наук, доцент, кафедра автоматизованих систем управління.
Email: olha.y.fedevych@lpnu.ua; https://orcid.org/0000-0003-4561-3874

Цитування за ДСТУ: Сікора Л. С., Лиса Н. К., Павлюк О. М., Сабат В. І., Федевич О. Ю. Інформаційні та логіко-когнітивні підходи до формування кібербезпеки техногенних інфраструктур з урахуванням рівня ризиків. Науковий вісник НЛТУ України. 2023, т. 33, № 1. С. 71–81.
Citation APA: Sikora, L. S., Lysa, N. K., Pavluk, O. M., Sabat, V. I., & Fedevych, O. Yu. (2023). Information and logical-cognitive approaches to the formation of cybersecurity of ecotechnogenic infrastructures of the region taking into account the level of risks. *Scientific Bulletin of UNFU*, 33(1), 71–81. https://doi.org/10.36930/40330110

Визначати рівень загроз за рахунок низького рівня управлінської підготовки відповідно призводить до розвалу інфраструктури (краю, держави та локальних систем) в умовах дії активних агресивних загроз структурного, ресурсного, інформаційного типу, які неможливо прогнозувати в термінальному часі циклі управління.

Проблемна ситуація полягає в тому, що в сучасних методах управління недостатньо використовуються логіко-когнітивні моделі особи, яка приймає рішення (когнітивний інтелектуальний агент), а тим більше мало приділено уваги формуванню команд для ефективного управління в умовах загроз (когнітивні компоненти кібербезпеки техногенних структур з ієрархією в умовах інтеграції протистояння атакам).

Об'єкт дослідження – формування кібербезпеки ієрархічних інфраструктур з врахуванням рівня ризиків.

Предмет дослідження – методи і засоби формування кібербезпеки ієрархічних інфраструктур з урахуванням рівня ризиків як підстави для прийняття цілеорієнтованих рішень в умовах дії загроз та інформаційних атак.

Мета роботи – розробити концепцію кібербезпеки (безпеки процесу управління в сенсі Н. Вінера) ієрархічних інтегрованих систем в умовах дії комплексу активних загроз.

Для досягнення зазначеної мети визначено такі основні *завдання дослідження*:

1) Обґрунтувати когнітивні засади координації та інформаційне забезпечення процесу формування і прийняття рішень.
2) Розробити інформаційну технологію експертного аналізу для інтелектуального оброблення даних в умовах дії загроз.
3) Обґрунтувати логіко-когнітивний метод експертного аналізу ситуацій для протидії інформаційним атакам.

Аналіз останніх досліджень та публікацій. Проблеми побудови процедур прийняття ефективних управлінських рішень у технічних та економічних системах досліджено у роботах [13, 19]. Теорії організації великих систем присвячена праця [12] в якій розглянуто базові моделі побудови структури, моделей функціонування, стратегії відкритого управління, ресурсні і стратегічні ігри, проблеми ефективного проектування. У працях [7, 16] розглянуто методи обробляння, класифікації та прогнозування даних як підстави для формування процесу прийняття рішень. Методи теорії експертних систем для використання у складних системах під час формування управлінських рішень розглянуто в працях [1, 3, 6]. Теорію координації у процесах управління розглянуто у праці [24], когнітивні технології оцінювання – в роботі [22], моделі ризиків у формуванні інтелектуальних стратегій – у роботі [23]. Метод активності інтелектуального агента на основі онтології розглянуто у праці [8]. У роботі [4] розглянуто проблему управління в умовах зміни ситуації під впливом порушень процесу прийняття рішень. У праці [15] обґрунтовано методи системного аналізу процесу прийняття рішень у соціальних, організаційних і технологічних структурах. У роботі [11, 18] розкрито методи проєктування складних систем і захист їх від атак та стратегічну безпеку системи. У монографії [25] розглянуто типи інформаційних війн. Результати досліджень, використаних у книгах [2, 18, 26] присвячені аналізу інформаційних технологій, концепції їх розвитку, платформам і стандартам, програмному забезпеченню і експертним системам, нечіткій логіці. У монографіях [2, 5, 14, 20, 21] розглянуто логіко-когнітивні методи прийняття рішень в умовах загроз.

Результати дослідження та їх обговорення / Research results and their discussion

Виклад основного матеріалу з проблеми управління складними системами в умовах дії ресурсних загроз та інформаційних атак. На підставі системного аналізу та їх інформаційних і логіко-когнітивних технологій необхідно визначити й обґрунтувати моделі-індикатори виявлення причин кризових та аварійних ситуацій у складних техногенних інтегрованих системах з ієрархічною інфраструктурою, що є важливою проблемою забезпечення стійкого функціонування енергоактивного об'єкта інфраструктури. За дії загроз та атак на процес і цілі управління кожної із інфраструктур споріднених виробництв, важливим засобом їх стійкості є інтеграція, як ресурсних інформаційних, інтелектуальних компонент для вироблення стратегічної лінії протидіям загрозам, що потрібно для забезпечення ефективних методів протидії та високого рівня кібербезпеки.

Когнітивні засади інформаційного забезпечення необхідні для побудови процедури та алгоритмів логічних ситуаційних висновків при неповних даних про динамічний стан технологічних систем в умовах загроз, є основою для побудови тестів відбору персоналу та повірки на справність системи АСУ.

Сучасний стан розвитку технологій управління складними об'єктами в інфраструктурі інтегрованих ієрархічних систем характеризується наявністю:

- автоматизованих систем управління технологічними процесами в агрегованих енергоактивних технологічних об'єктах, що входять у структуру як компоненти з певним (фізико-термодинамічним, енергетичним, ресурсним, електротехнічним, інформаційно-управляючим) призначенням згідно з типом виробництв;
- загальної інфраструктури ієрархії управління (агрегатний контроль, оперативне управління, адміністративно-фінансове, локально тактичне і стратегічне командне управління нижнього рівня ієрархії);
- цілеорієнтованого управління з координаційними стратегіями узгодження корпоративних правилами поведінки під час формування локальних і глобальних цілей;
- системи комплексу методів, засобів кібербезпеки.

Відповідно до цілей виробництва та зовнішньої ситуації, в якій перебуває досліджувана інфраструктура з комплексом управління, потрібно визначити ролі і способи поведінки (АСУ) автоматизованої системи управління у взаємодії з командою оперативного управління (конструктивними агентами). Необхідно оцінити системну взаємодію на всіх рівнях інфраструктури:

- IS_1 – комбінованих людино-машинних інтегрованих систем оперативного управління комплексом об'єктів і агрегатів;
- $IS_{2,1}$ – оперативно-адміністративного стратегічного цілеорієнтованого управління на всіх рівнях ієрархії просторової інфраструктури;
- $IS_{2,2}$ – координаційного управління інтегрованою інфраструктурою в системах державного та приватного виробництва;
- IS_3 – систем оперативного цілодобового управління режимом та сервісним обслуговування технологічних об'єктів.

Це вимагає від персоналу для протидії загрозам високого рівня фахової підготовки, інтелектуальної психологічної стійкості, професіональної зрілості.

У критичний для прийняття рішень момент контролю та управління, за дії загроз та атак на інфраструктуру, персонал повинен мати відповідну до вимог цілеорієнтовану і мотивовану поведінку, яка залежить від когнітивних здібностей осіб та їх інформативності і повноважень. За когнітивними характеристиками можна виокремити такі базові типи мислення оперативного працівника, які необхідні йому під час ефективного і конструктивного опрацювання даних, формування управлінських рішень на протидію загрозам:

- $КМ_1$ – зі сценарною уявою розвитку подій у системі й образним мисленням у формуванні рішень на основі підсвідомо набутих знань і професійного досвіду;
- $КМ_2$ – з аналітичним структурованим мисленням, що ґрунтується на аналізі подій, синтезу стратегій і планів дій з використанням упорядкованих базових знань про структуру і динаміку, мету функціонування ієрархії та кожного агрегата технологічної системи;
- $КМ_3$ – креативне логіко-системне мислення характеризує здатність до інтегрованого підходу у формуванні рішень у граничних і аварійних режимах, пошук нестандартних рішень для стабілізації функцій інтегрованої інфраструктури і її кібербезпеки.

Відповідно на верхньому рівні ієрархії рішення повинні формувати особи другого типу $КМ_2$, але в разі нечіткості і неповноти даних про ситуацію на різних рівнях ієрархії як від інформаційних систем АСУ-ТП, так і операторів лабораторного контролю, потрібно залучати експертів з третім типом мислення. Ці особи з високим рівнем інтелекту забезпечують повноту аналізу даних про ситуацію завдяки високому рівню знань, спроможності моделювати й інтерпретувати ситуацію в ієрархії, формувати оперативні дії для недопущення аварійних ситуацій на об'єктах, блоках, агрегатах технологічних систем (рис. 1). Функціональну стійкість ієрархії у кризових ситуаціях в інтегрованій інфраструктурі можуть забезпечити оперативні працівники з управління з креативним мисленням {$КМ_1$, $КМ_2$, $КМ_3$}, які є базовою командою цілеорієнтованого управління процесом та кібербезпекою інфраструктури.

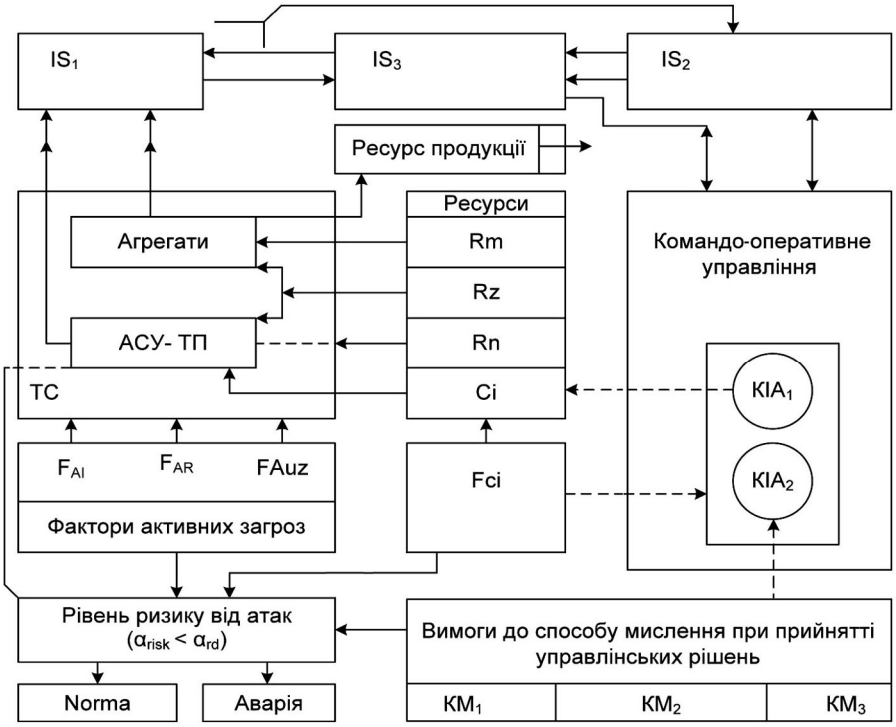

Рис. 1. Системно-інформаційна взаємодія загроз і (АСУ – когнітивний агент) / Systemic-information interaction of threats and (ACS – cognitive agent)

На рис. 1 введено такі позначення: IS – ієрархічна структура; Ci – цілі; $\{F_i\}$ – фактори збурень; KIA – когнітивний інтелектуальний агент; $\{КМ_i\}$ – когнітивний тип мислення; α_r – рівень ризику аварійної ситуації; $\{R_i\}$ – ресурсні потоки. Наведена схема системно-інформаційних загроз є підставою для побудови категорних логіко-когнітивних діаграм управлінських потоків даних і взаємодії. Адже, загрози інформаційній безпеці мають системний характер і містять: загрози безпеці інформації та інформаційній інфраструктурі; загрози безпеці суб'єктів інформаційної сфери й соціальних зв'язків між ними від інформаційних впливів; загрози належному порядку реалізації прав та інтересів суб'єктів інформаційної сфери.

Експертний аналіз ситуації при дії загроз на процес управління. Інтелектуальні операції у процедурах прийняття цільових рішень є підставою для побудови процедур оцінювання змісту ситуації в цільовому просторі системи та режиму функціонування енергоактивного об'єкта в умовах граничних навантажень, за яких некоректне трактування призводить до виникнення аварій або екстремальних ситуацій і психічного перевантаження оперативного персоналу. Поняття "загроза" є спорідненим із поняттям "небезпека", яка створює умови заподіяння або реально завдає шкоду не тільки інформаційним відносинам досліджуваної діяльності, але й усій інформаційній безпеці: це може бути як порушення цілісності інформації, подання невідповідної інформації, так і викрадення службової інформації, що спричиняють конкретну шкоду, наприклад, у вигляді прийняття неправильного управлінського рішення, ведення інформаційної війни чи дезінформацію.

Найскладнішим елементом процесу управління є інтелектуальні дії з обробляння інформації та прийняття управлінських рішень оператором (когнітивним агентом). Інформаційні системи у складі АСУ-ТП мають

бути орієнтовані для відбору нестандартних оперативних і технологічних даних від ієрархічної структури, їх алгоритмічного опрацювання та класифікації за заданими ознаками, що забезпечує команді (агентів-управлінців) інтелектуальну базу формування стратегій виходу із кризи на підставі креативного перебору допустимих стратегій з використанням інформаційних та інтелектуальних комбінацій операцій.

У складних системах з ієрархічною інфраструктурою, за командного методу прийняття рішень на оперативному, адміністративному та стратегічному корпоративному рівнях, в умовах дії загроз інформаційних активних атак, використовують системи підтримки прийняття рішень (СППР) на цілеорієнтоване управління.

Системи СППР залучають у свою структур експертів, які на підставі інженерії знань для кожної предметної області формують базу знань, необхідні для підтримки прийняття рішень в діалоговому режимі реалізації управління в кризових умовах і надзвичайних ситуаціях функціонування інфраструктури.

Відповідно експерти мають спеціалізуватись за напрямами знань і технологій – ресурсних, агрегатно-технологічних, оперативного управління та інформаційно-вимірювальних системах, адміністративного та стратегічного керування.

Координаційне управління у складних техногенних ситуаціях виникнення загроз та аварій ґрунтується на командних методах прийняття рішень експертами під керівництвом лідера, який в режимі діалогу із стратегічним рівнем ієрархії на підставі оцінки ситуації вживають заходів для ліквідації загроз.

Інтелектуальне мислення та операції формування стратегічних цілеорієнтованих координаційних рішень забезпечує відповідні експертні оцінки:

- оброблення логіко-когнітивна образів ситуацій, сформованих на підставі інформаційних технологій, для оцінювання стану системи у просторі цілей;
- аналіз сценарію розвитку подій відносно цільового стану системи та визначення міри відхилення;
- на підставі міри розходження формують процедуру синтезу стратегій, тактики і плани дії, які переводять в команди послідовних цільових дій;
- на підставі оцінення зміни ситуацій у разі недосягнення цілей переходять до координаційних стратегій.
- Інформаційні операції в процедурах формування рішень на управління ІАСУ:
- оброблення потоків даних інформаційно-алгоритмічна, для оцінення ситуацій у просторі станів та побудови образу ситуацій в енергоактивному об'єкті;
- аналіз траєкторії поведінки параметрів режиму об'єкта відносно заданих координат завантаження і продуктивності;
- визначення міри відхилення траєкторії стану від заданої режимної;
- у разі недосягнення цільової області завдяки реалізованій стратегії, за умови наближення до граничного режиму, оцінюють нову ситуацію як нестандартну.

Термінальна протидія атакам на ієрархію інфраструктури з енергоактивними об'єктами визначається на інтервалах часу в циклі управління, на яких формуються та здійснюються атаки на процеси управління інфраструктурою.

Згідно з цільовими завданнями, виробнича система охоплює управлінські рівні ієрархії, технологічної агрегованої структури енергоактивної системи (рис. 2):

- агрегована технологічна лінія, в якій відбувається процес виробництва продукції (автоматизоване управління, АІА);
- (ІВС) – інформаційно-вимірювальна система для відбору даних і передачі в АСУ-ТП для формування команд управління (автоматичний режим);
- автоматична система управління технологічним процесом (АСУ-ТП);
- блок оперативного управління з дисплейним і щитовим комплексом відображення інформації та засобами і механізмом для виконання управлінських та координаційних команд (людський ресурс, БОУ-МК);
- блок адміністративно-технологічного управління виконанням виробничих планів (людський ресурс, БА-ТУ);
- блок стратегічного управління з використанням оперативної та експертної підтримки (людський ресурс високого рівня, БСУ);
- інформаційної моделі виробничого процесу, як бази формування управлінських рішень згідно з динамічною ситуацією (еталон функціонування ВС, бази даних і знань, СППР, експерти).

Відповідно до структури системи і цільових задач формуються технології придбання і використання знань для розв'язування задач управління в АСУ-ТП в автоматичному й оперативному режимах (рис. 2).

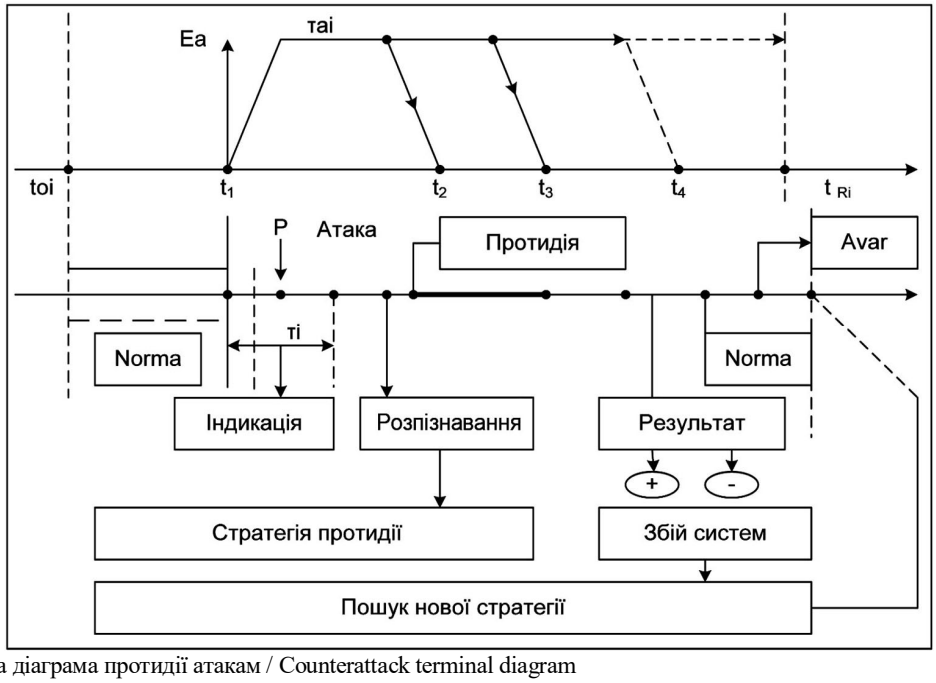

Рис. 2. Термінальна діаграма протидії атакам / Counterattack terminal diagram

Відповідно інфраструктура виробничих комплексів може містити певну кількість технологічних систем з відповідним корпоративним управлінням, які об'єднанні типом продукції, приорітетами на зовнішньому ринку, стратегічними цілями, фінансовими ресурсами, що забезпечує їм виробничу, функціональну стійкість на міжсистемному рівні. Відповідно експертний аналіз на термінальному інтервалі проводиться згідно з діаграмами протидії атакам на інтервалі.

Відповідно до цільового завдання для відбиття кібератак на інфраструктури використовується колектив експертних систем (експертів) для вироблення протидії загрозам (рис. 3), в який входять відповідні особи, спеціалізовані за напрямами комплексу знань:

- захист ресурсів;
- експерт зі структуризації агрегатів технологічної лінії;
- експерти з інформаційно-вимірювальних систем та оброблення даних;
- експерти з оцінення ситуацій та виявлення індикаторів з можливих типів загроз (управління, ресурсні атаки, інформаційні та інтелектуальні, логіко-системні, когнітивні і психологічні);
- експерти стратегічного управління цілеорієнтації;
- експерти з інтеграційних координаційних методів у вирішенні проблем кібербезпеки інтегрованої інфраструктури.

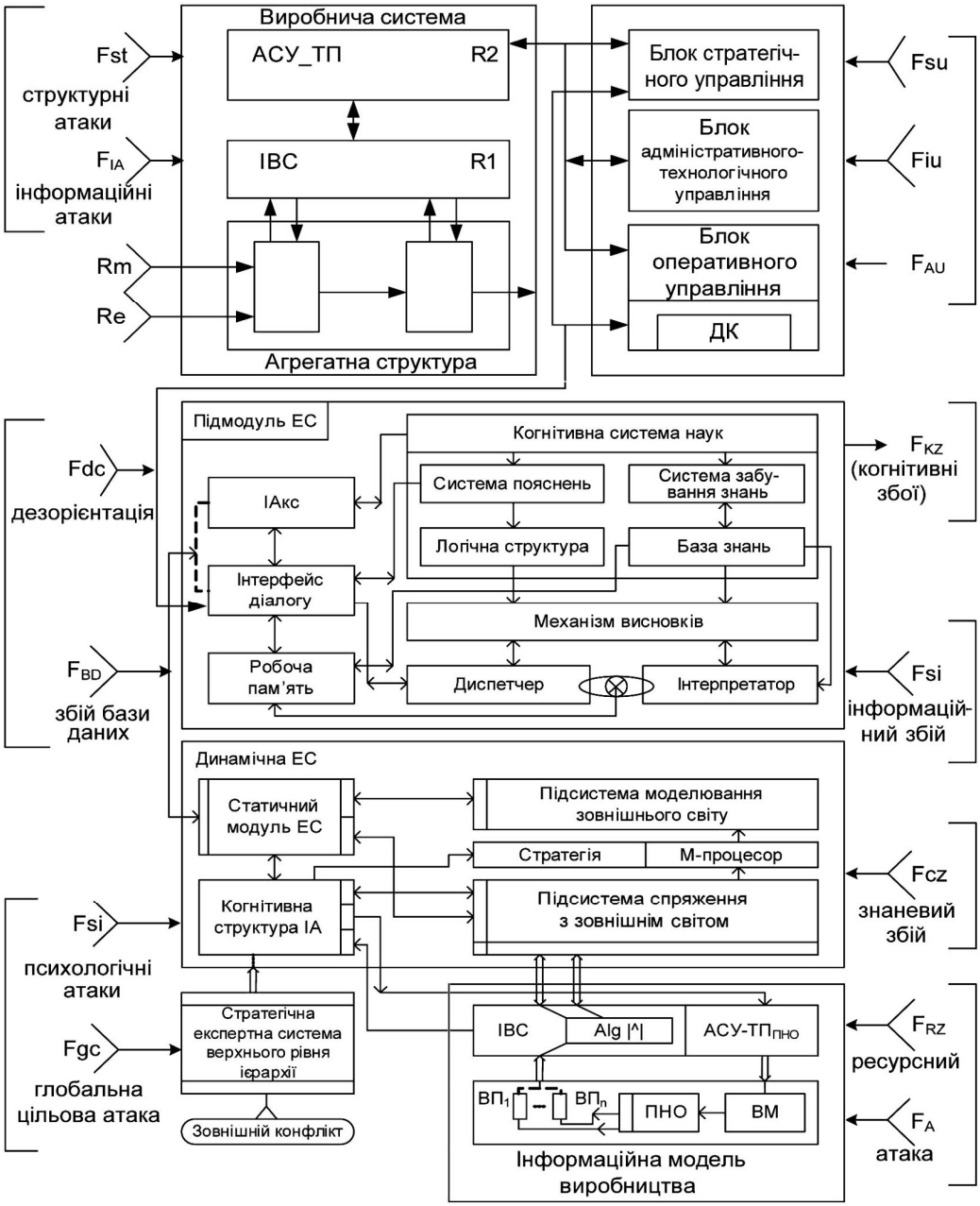

Рис. 3. Схема ієрархії колективу експертних систем управління виробничою структурою з потенційно небезпечними агрегованими об'єктами інфраструктури / The scheme of the hierarchy of the team of expert management systems of the production structure with potentially dangerous aggregated infrastructure objects

На рис. 3 введено такі позначання: фактори загроз (Fsu…….Fsz), ПНО – потенційно-небезпечний технологічний активний об'єкт (реактор); ВП – вимірювальний перетворювач; ВМ – виконавчий механізм; IBC – інформаційно-вимірювальна система; АСУ-ТП – автоматична система управління технологічним процесом; ЕС – експертна система; ІА – інтелектуальний агент-експерт; ІАкс — команда інтелектуальних агентів експертів, $\{\tau_i\}$ – фактори активних атак на систему АСУ, атаки $< F_{ые...}F_{gS} >$ – ресурсні та інформаційні.

Ієрархії інформаційного й інтелектуального забезпечення містять такі виконавчі структури, які реалізують процес управління і прийняття обґрунтованих управлінських рішень:

- структура виробничої системи, в яку входить агрегована структура об'єкта управління, інформаційно-вимірювальна система (ІВС), автоматизована система управління технологічним процесом (АСУ-ТП) і відповідно трирівнева система оперативного управління, адміністративного технологічного управління та стратегічного управління, яка пов'язана з експертною системою підтримки прийняття рішень;
- структура експертної системи, яка містить підмодуль логічного виводу і підмодуль динамічної експертної системи, при цьому процес прийняття рішень опирається на когнітивну впорядковану логічну структуру системи технічних наук та на логічний блок (система пояснень, логічна структура побудови висновків, бази знань та інтерпретатора знань);
- структура експертного забезпечення управління, динамічний комплект експертної системи, когнітивна структура інтелектуального агента, як генератора стратегій для цільових рішень, якість якого залежить від інтелектуального рівня персоналу і їх креативності при прийнятті рішень в екстремальних ситуаціях;
- база даних і знань про виробничий процес і його структурна організація.

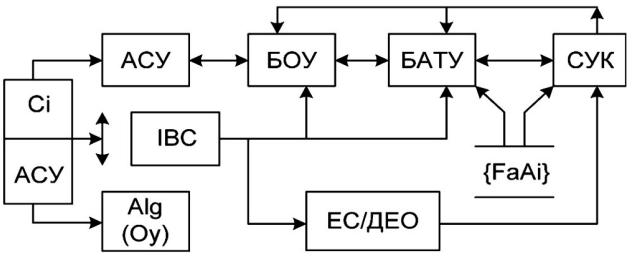

Рис. 4. Категорна діаграма процесу інтелектуального управління (АСУ-КІ) / Categorical diagram of the process of intelligent control (ACS-CI)

Позначення до категорної діаграми процесу управління (рис. 4): {Ci} – цілі системи, АСУ – система автоматизованого управління, БОУ – базовий об'єкт управління, ЕС/ДЕО – експертна система з базою знань для експертної оцінки ситуацій, (БАТУ) – блок автоматичного технологічного управління об'єктом, $СУ_R$ – система координації рішень.

Інформаційне та інтелектуальне забезпечення процесу оброблення потоків даних для експертних висновків про динаміку об'єкта та вибір стратегій цілеспрямованого управління. У технологічних структурах неможливе управління процесами без відбору даних, їх опрацювання, а в разі неповноти – поповнення завдяки знанням експертів. Розглянемо етапи функціонування експертної системи, бази знань управління, що формуються внаслідок сукупності знань і обізнаності виробничого й управлінського персоналу, їх інтелектуальних дій на основі комплексу операцій (рис. 5):

Етап 1. Формування стратегічного цільового завдання;

Етап 2. Вибір стратегій режиму ЕС для конкретної предметної області;

Етап 3. Ідентифікація, у процесі якої групуються задачі на класи, які необхідно вирішити насамперед для уточнення цільових завдань та виявлення факторів ризику;

Етап 4. Концептуалізація, в ході якої проводиться змістовний аналіз предметної області, яка пов'язана з технологією виробництва;

Етап 5. Виділення основних понять та їх взаємозв'язків, визначення методів і стратегій розв'язання задач, які виникають у ході технологічного процесу в реальному часі;

Етап 6. Формалізація, тобто вибираються мови подання даних і задач, програмні засоби, розробляються способи представлення знань;

Етап 7. Формалізація основних понять, що забезпечує сприйняття ситуації оперативним персоналом;

Етап 8. Розроблення правил структуризації ієрархічної організації інфраструктури.

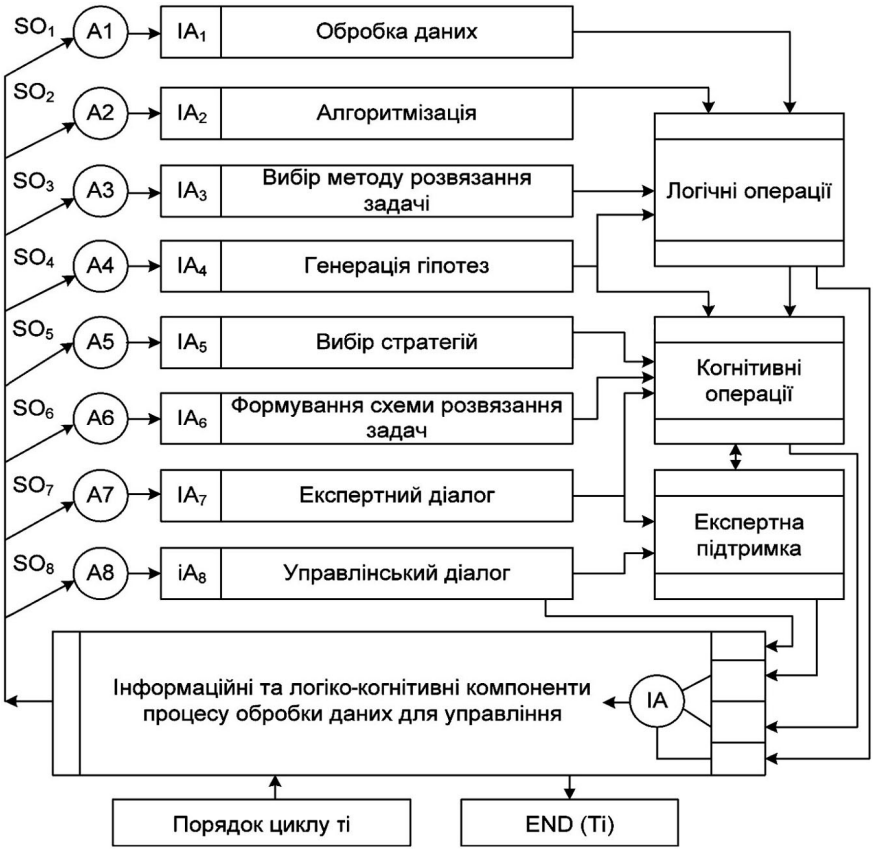

Рис. 5. Діаграми логіко-когнітивних процедур оброблення даних від об'єктів з використанням інформаційних технологій та множини системних операцій (SOi) / Diagrams of logical-cognitive procedures for processing data from objects using information technology and a set of system operations (SOi)

Отже, роль особи зводиться до того, що експерт:

- $ІА_1$ – обробляє дані і знання предметної області;
- $ІА_2$ – відповідно до цільової задачі і вибирає схему, процедуру, алгоритм та стратегію її розв'язання на основі ідентифікації факторів ризику;
- $ІА_3$ – недостатності даних і неповноти знань здійснює пошук методів їх доповнення знань у межах базової теорії;
- $ІА_4$ – основі евристик генерує гіпотези про схеми розв'язання задачі;
- $ІА_5$ – вибирає процедури або алгоритми, згідно з еталонними моделями функціонування виробничої системи та цілеорієнтованих стратегій;
- $ІА_6$ – знаходження відповідної схеми розв'язання задачі (проблеми), експерт описує проблемну область у вигляді сукупності фактів і правил (доведення, розв'язання);
- $ІА_7$ – наповнює ЕС новими знаннями (як основу процесу самонавчання ЕС);
- $ІА_8$ – передає дані оперативному персоналу для формування рішень. Відповідно, розробляється з відповідною послідовністю до цільової задачі і проблемної ситуації, відповідні етапи пошуку методу розв'язання задач управління в діалоговому режимі;
- $ІА_9$ – генерація стратегічних і локальних цілей функціонування інфраструктури.
- R_1 – Режим ЕС консультації клієнт – ІА: під час діалогу оператора-інтелектуального агента (ІА) з ЕС забезпечується розв'язання задачі з предметно-орієнтованої області, використовуючи сформовану базу знань і БД, СД-ЕС, та ситуаційні дані певного рівня достовірності.

Режим усвідомлення ЕС власної сутності знаннєвої компоненти через самотестування містить процедури прийняття рішень на основі схем логічного пояснення, механізми схеми, процедури доведення при розв'язанні тестових задач (самодіагностика) у структурі виробничої системи – системи, що бере участь у стратегічному управлінні.

Основні концепції викладені на схемах відповідно до цільової задачі стійкого цілеорієнтованого управління інфраструктурою та у табл. 1. Позиції (V_{ij}) – компоненти інформаційних вимог і ознак інтеграції інфраструктури. На підставі цієї таблиці, розробленою командою експертів, які відповідають кваліфікаційним вимогам, що забезпечують процедури інтеграції системи на всіх рівнях, побудуємо категорну схему ризиків, які виникають при допущених помилках процедури інтеграції. Оскільки системи ієрархічного типу в сенсі структури стратегії управління ресурсних і фінансових можливостях не є однорідними, то забезпечити ефективність управління складно, виходячи з точки зору можливості сформувати команди управлінців, які були б не конфліктними та професійно однорідними. Це дало би змогу забезпечити безконфліктну управлінську діяльність в умовах дії загроз на підставі визначення міжкомандного лідера.

Табл. 1. Відповідність системних ознак вимогам за даними інтеграції в системі управління / Compliance of system features with the requirements of specified integration in the management system

П/П	Інтеграційні вимоги	Інтеграційні ознаки	
1. Цільова інтеграція			
V 1.1	Всефакторна визначеність цілей	V2.1	Диспозиція цілей враховує внутрішні і зовнішні фактори впливу на їх визначення
V 1.1a	Несуперечливість і взаємоузгодженість цілей	V2.1a	Цілі структуровані внаслідок декомпозиції
2. Функціональна інтеграція			
V 1.2	Узгодження функцій з цілями управління	V2.2	Функціональне структурування системи відповідає цільовому на основі декомпозиції
V 1.2a	Усунення дублювання функцій управління	V2.2a	Виконане згортання функцій управління на основі
3. Організаційна інтеграція			
V 1.3	Узгодженість організаційної структури управління з цільовою і функціональною структурами	V2.3	В організаційних елементах системи (у підрозділах, підсистемах) закріплені цілі, локалізовані функції управління та визначені цільові і функціональні завдання.
V 1.4	Регламентація і міжелементна узгодженість дій у процесі управління.	V2.4	Виконані розподіл і закріплення (з урахуванням координації) за організаційними елементами дій, які виконуються в процесах прийняття і реалізації рішень у системі управління.
V 1.5	Забезпечення пропускної спроможності елементів системи управління	V2.5	Розподіл навантаження на елементи системи оптимізований
V 1.6	Стійкість системи управління до деструктивних впливів	V2.6	Встановлений контроль за параметрами інтеграції системи та розроблені заходи протидії дезінтеграції
4. Когнітивна процедурна активізація			
V 1.7	Актуалізація змін у ході функціонування системи	V2.7	Розроблені процедури авторегуляції і реінжинірингу системи з урахуванням контрольованих параметрів інтеграції
V 1.8	Професійні і когнітивні якості розробників і виконавців інтегрованих рішень	V2.8.	Професійна відповідність і когнітивна сумісність персоналу досягнуті, що дає змогу приймати і реалізовувати інтегровані рішення.
5. Інформаційна інтеграція			
V1.9	Узгодженість інформаційної структури з цільовою, функціональною, організаційною структурами ("інфораструктурне" позиціювання)	V2.9	Інформаційна структура забезпечує концентрацію і локалізацію інформації в елементах цільової, функціональної, організаційної структур
V1.10	Спільне використання інформації в системі управління	V2.10	Наявність єдиної інформаційної бази даних, відповідної функціональним потребам управління
V1.11	Усунення недоцільного дублювання інформації в системі управління	V2.11	Мінімально необхідний рівень дублювання інформації
V1.13	Сумістність інформації в елементах системи управління	V2.13	Забезпечене перетворення неоднорідної інформації в однорідну на зіставність даних
V1.14	Агрегування інформації про хід і результати діяльності, стан системи управління	V2.14	Наявність облікових методів і засобів синтезу й узагальнення даних про функціонування системи
6. Економічна інтеграція			

V1.15	Узгодженість структур системи управління і показників економічної результативності діяльності суб'єкта господарювання	V1.15	Показник економічного ефекту й ефектоформувальні показники структуровані відповідно до структурної будови системи управління та застосованої концепції управління і репрезентативні для визначення стану суб'єкта господарювання.
V1.16	Оцінка ризиків інтеграції	V 2.16	Система економічних показників ієрархічно впорядкована, вертикально і горизонтально позиціонована та прийнятна для скоординованого управління економічною результативністю
V1.17	Забезпечення економічної доцільності дій в управлінському процесі з досягнення економічно ефективної результативності діяльності суб'єкта господарювання	V2.17	Наявні методи і засоби інтелектуалізації дій ("економіки знань") з економічного обґрунтування управлінських рішень щодо впливу на економічний ефект і стан суб'єкта господарювання
7. Інструментально-прикладна інтеграція управління			
V1.18	Наскрізність процесу управління за рівнями управління на основі уніфікації і стандартизації процесів перетворення інформації	V2.18	Досягнуто типовості, модульності та не дублювання інформаційних технологій
V1.19	Безпека процесів зберігання і перетворення інформації. Сумісність процесів прийняття і реалізації рішень	V2.19	Наявні засоби контролю і захисту інформації та процесів її перетворення
V1.0	Можливість виникнення конфліктів	V2.20	Наявні засоби інформаційних технологій проєктування рішень, відстеження їх виконання на єдиній базі проєктно-виконавської інформації із застосуванням уніфікованих інформаційно-процесних технологій

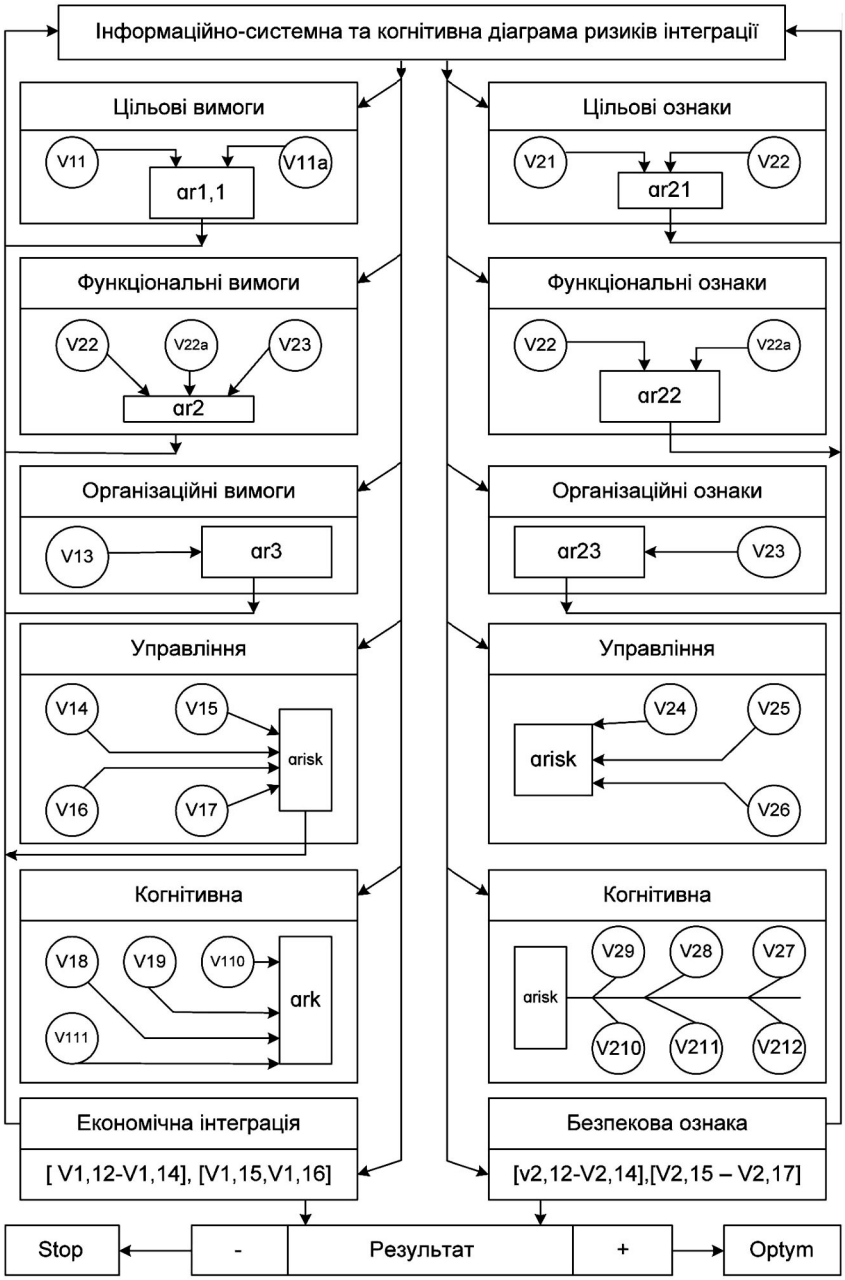

Рис. 6. Схема ризиків за неузгодження вимог інтеграції систем / Risk scheme in case of inconsistent requirements for the integration of systems

Табл. 2. Основа експертного аналізу у реальному часі / The basis of real-time expert analysis

Тип стану	Зміна ефекту діяльності	Зміна ступеня інтеграції	Оцінення складових комплексного стану	
			Економічний стан	Інтеграційний стан
1.1	$\alpha_{r1} < \alpha_d$	$\alpha_{r1} < \alpha_d$	Планово досягнутий	Планово досягнутий
1.2	$\alpha_{r2} \le \alpha_d$	$\alpha_{r2} < \alpha_d$	Послаблений стан за планово досягнутого стану інтеграції	Планово досягнутий, але із застереженням про приховану дезінтеграцію
1.3	$\alpha_{r3} \le \alpha_d$	$\alpha_{r3} \le \alpha_d$	Підсилений стан за планово досягнутого стану інтеграції	Ефективний планово досягнутий стан
1.4	$\alpha_{r4} = \alpha_d$	$\alpha_{r4} > \alpha_d$	Плановий стан в умовах послабленого стану інтеграції	Послаблений стан за явної дезінтеграції, який загалом не вплинув на економічний стан
1.5	$\alpha_{r5} \ge \alpha_d$	$\alpha_{r5} \ge 2\alpha_d$	Плановий стан за послабленого стану інтеграції	Послаблений стан за явної дезінтеграції, який негативно вплинув на економічний стан
1.6	$\alpha_{r6} \le \alpha_d$	$\alpha_{r6} \le 2\alpha_d$	Підсилений стан в умовах послабленого стану інтеграції	Послаблений стан за явної дезінтеграції, який не перешкодив підсиленню економічного стану
1.7	$\alpha_{r7} < \alpha_d$	$\alpha_{r7} < 0{,}5\alpha_d$	Плановий стан за підсиленого стану інтеграції	Підсилений стан, який не забезпечив підсилення економічного стану
1.8	$\alpha_{r8} \ge 3\alpha_d$	$\alpha_{r8} \to \max$	Послаблений стан за неефективного підсилення стану інтеграції	Підсилений стан, який негативно вплинув на економічний стан внаслідок прихованої дезінтеграції
1.9	$\alpha_{r9} \le 0.5\alpha_d$	$\alpha_{r9} \to \min$	Підсилений стан в умовах підсиленого стану інтеграції	Підсилений стан, який позитивно вплинув на економічний стан.

Оцінення можливих ризиків комплексного стану на основі комбінації типу діяльності і ступеня інтеграції ґрунтується на табл. 2, яка сформована на основі експертного аналізу в реальному часі виробництва та подій у зовнішньому середовищі в умовах конкурентної боротьби.

Обговорення результатів дослідження. У сучасних виробничих і соціокомунальних структурах, системах телекомунікації і зв'язку й управління складними системами з ієрархічною організацією, причинами виникнення екстремальної та аварійної ситуацій можуть бути закладені помилки в проєктах та відповідно в цілях і стратегіях. Активні атаки, збої, неполадки (зниження надійності і ресурси) призводять до збою функціонування. Якщо на агрегатному рівні виробництва виникають проблеми підвищення функціональної надійності, то відповідно на верхніх рівнях ієрархії управління атаки збоїв інформаційного і когнітивного типу і загрози призводять до аварій. Інтелектуальні і когнітивні помилки оперативного персоналу стають причиною катастроф і надзвичайних ситуацій, за яких система втрачає цільову функціональність, а інформаційна і цільова дезорієнтація персоналу стратегічного рівня руйнує інфраструктуру.

Відповідно до цілей системи сформовано вимоги до надійності і функціональності агрегатів, АСУ, структури управління, які враховують можливі типи загроз і атак. Знаннєві інтелектуальні та когнітивні характеристики оперативного персоналу та способу їх мислення визначають здатність приймати стратегічні креативні рішення в умовах надзвичайних ситуацій.

Кібербезпека, як стратегічна безпека управління інфраструктурою складної ієрархічної системи, є актуальною проблемою забезпечення функціональної стійкості згідно з цільовими завданнями і ґрунтується на високоякісному інформаційному та інтелектуальному забезпеченні оцінки ситуацій під час формування прийняття і реалізації цілеорієнтованих рішень в умовах дії загроз, ресурсних і структурних та інших типів атак на інфраструктуру. Основи теорії кібербезпеки було закладено в період 1956-1975 рр. у працях українських учених О. Г. Івахненка, В. М. Глушкова, Д. Рабіновича щодо проблем енергетики, металургії.

Отже, за результатами виконаної роботи можна сформулювати такі наукову новизну та практичну значущість результатів дослідження.

Наукова новизна отриманих результатів дослідження:

1. На підставі системного аналізу та теорії ієрархічних структур обґрунтовано когнітивні засади координації та інформаційне забезпечення процесу формування і прийняття рішень в умовах дії атак на термінальних інтервалах часу функціонування інфраструктури та протидії активним загрозам різного типу на структуру і динаміку та цілі управління.
2. Обґрунтовано логіко-когнітивний метод експертного аналізу ситуацій в АСУ за дії загроз та інформативних атак для прийняття ефективних, робастних рішень для цілеорієнтованого управління і кібербезпеки на основі знань висококваліфікованих експертів, які мають високу наукову і виробничу кваліфікацію і великий професійний досвід у цій галузі.
3. Розроблено метод інтелектуального оброблення даних для оцінювання ситуацій в об'єкті управління за дії структурних та інформаційних загроз та атак на АСУ з використанням логіко-когнітивних методів вибору способу прийняття цілеорієнтованих рішень з використанням комплексних методів кібербезпеки інфраструктури.

Практична значущість результатів дослідження – розроблено метод оцінювання ефективності інформаційних, когнітивних та інтелектуальних операцій під час формування управлінських рішень в умовах дії активних загроз і комплексних атак на основі використання знань висококваліфікованих експертів. Метод можна використати для створення тестів відбору управлінських кадрів для верхнього рівня ієрархії інфраструктури корпоративних, організаційних та інших галузей виробництва, які забезпечили би мінімізацію ризиків в екстремальних умовах

Висновок / Conclusions

Розроблено концепцію кібербезпеки (безпеки процесу управління в сенсі Н. Вінера) ієрархічних інтегрованих систем в умовах дії комплексу активних загроз та інформаційних атак, що дало змогу розробити метод інтелектуального оброблення даних для оцінювання ситуацій в об'єкті управління. Згідно з цільовим завданням розроблення методів розв'язання задач кібербезпеки інфраструктури:

- проаналізовано літературу з проблем кібербезпеки техногенної інфраструктури, стійкості до атак і відновлювальності в умовах дії загроз;
- обґрунтовано задачі, які необхідно розв'язати для забезпечення протидії системи управління атакам і загрозам на інфраструктуру і систему, стратегії цільового управління;
- обґрунтовано когнітивні засади інформаційного забезпечення, необхідного для створення стратегій активної протидії атакам на управлінську структуру на підставі стратегій координації і цілеорієнтації;
- проведено експертний аналіз виникнення ситуацій за дії загроз та побудовано діаграму операцій виявлення та протидії атакам;
- обґрунтовано інформаційне забезпечення методів обробляння потоків даних для визначення індикаторів ознак експертною системою як підстави стратегії протидії загрозам;
- проаналізовано процес взаємодії оперативної і цільової, когнітивних та автоматизованих рівнів прийняття рішень ієрархії управління;
- обґрунтовано системну концепцію процесів інтеграції і структури координації цілеорієнтованого управління.

Розв'язання наведених вище проблемних задач на системному та інформаційному рівнях може допомогти в модернізації наявної інфраструктури та покращити процес їх проєктування для підвищення рівня комплексної кібербезпеки.

References

1. Barankevich, M. M. (2008). Expert methods in decision-making. Lviv: LNU named after Franka, 214 p. [In Ukrainian].
2. Belz, O. (2009). Basics of economic expert systems. Lviv: Center of LNU named after Ivan Franko, 238 p. [In Ukrainian].
3. Belz, O. (2009). Basics of economic expert systems. Lviv: LNU named after Franka, 238 p. [In Ukrainian].
4. Demri, S., Goranko, V., & Lange, M. (2016). Temporal Logics in Computer Science, Cambridge: Cambridge University Press, 752 p.
5. Durnyak, B. V., Sikora, L. S., Lysa, N. K., Tkachuk, R. L., & Yavorskyi, B. I. (2017). Information and laser technologies for the selection of data streams and their cognitive interpretation in automated control systems. Lviv: Ukrainian Academy of Printing, 644 p. [In Ukrainian].
6. Erina, A. M. (2004). Statistical modeling and forecasting. Kyiv: Nauka, 170 p. [In Ukrainian].
7. Hettmanserger, T. (1985). Statiskal inference Based on Ranks – New York, 2ws, 335 p.
8. Hovorushchenko, T., & Pavlova, O. (2019). Method of Activity of Ontology-Based Intelligent Agent for Evaluating the Initial Stages of the Software Lifecycle. *Advances in Intelligent Systems and Computing*. Vol. 836, 169–178. https://doi.org/10.1007/978-3-319-97885-7_17
9. Hrytsiuk, Y. I. (2022). Comprehensive software quality assessment system. *Scientific Bulletin of UNFU*, 32(2), 81-95. https://doi.org/10.36930/40320213
10. Hrytsiuk, Y. I. (2022). Features of giving preference to the characteristics of the software product quality model. *Scientific Bulletin of UNFU*, 32(3), 79-102. https://doi.org/10.36930/40320313
11. Khoroschko, V. O., Bobalo, B. Ya., & Dudykevich, V. B. (2020). Projecting of complex information protection systems. Lviv: "NU LP" Publishing House, 320 p. [In Ukrainian].
12. Kondratiev, V. V. (1989). Large systems: Modeling organizational mechanisms. Moscow: Science, 245 p. [In Russian].
13. Konstantinov, S. M., & Ponomarenko, Yu. L. (2010). Information technologies of modern enterprise management. Lviv: UAD, vol. 1, 368 p. [In Ukrainian].
14. Lysa, N. K. (2020). Information technologies for the creation of environmental monitoring systems of regional man-made structures. Lviv: Ukrainian Academy of Printing, 224 p. [In Ukrainian].
15. Lyugger, Dzh. F. (2003). Iskusstvennyy intellekt: strategiya i metody resheniya slozhnykh problem. Moscow: Vilyams, 864 p.
16. Mark, L. Davison. (1988). Multidimensional scaling. New York. IWss, 253 p.
17. Muschik, E., & Muller, P. H. (1990). Entschidun – gspraxis. Berlin VEB Verlog Technik, 206 p.
18. Mykytin, H. V., Dudykevich, V. B., & Bobalo, Y. Ya. (2019). Strategic security of the "object - information technology" system. Lviv: "NU LP" Publishing House, 580 p. [In Ukrainian].
19. Ponomarenko, V. S. (2002). Information systems and technologies in the economy. Kyiv: Academy, 542 p. [In Ukrainian].
20. Sikora, L. S. (2001). Robust and informative concepts in the procedures of the synthesis of the management system. Lviv: Ukrainian Academy of Printing, 577 p. [In Ukrainian].
21. Sikora, L. S., & Lysa, N. K. (2019). Information and laser technologies for the creation of environmental monitoring systems of energy-active man-made production structures. Lviv: Ukrainian Academy of Printing, 370 p. [In Ukrainian].
22. Sikora, L., Tkachuk, R., Lysa, N., Dronyuk, I., & Fedevych, O. (2020). Information and Logic Cognitive Technologies of Decision-making in Risk Conditions. IntellTSIS 2020. Proceedings of the 1st International Workshop on Intelligent Information Technologies & Systems of Information Security. Khmelnytskyi, Ukraine, 340–356. Retrieved from: http://ceur-ws.org/Vol-2623/paper29.pdf
23. Sikora, L., Tkachuk, R., Lysa, N., Dronyuk, I., Fedevych, O., & Navutka, M. (2020). Information technologies of formation of intellectual decision-making strategies under conditions of cognitive failures. 1st International Workshop on Computational & Information Technologies for Risk-Informed Systems (CITRisk – 2020). Cherson, Ukraine, vol. 2805, 233–254.
24. Sikora, L., Tkachuk, R., Lysa, N., Dronyuk, I., Fedevych, O., & Talanchyk, R. (2021). Information-resource and cognitive concept of threats influence identification on technogenic system based on the cause and category diagrams integration. IntellTSIS 2021. Proceedings of the 2nd International Workshop on Intelligent Information Technologies & Systems of Information Security with CEUR-WS Khmelnytskyi, Ukraine. Vol. 2853, 398–416.
25. Tsypanov, V. V., & Bukharin, S. M. (2007). Information wars in business and politics. Moscow: Academic project, 336 p. [In Russian].
26. Vendrov, A. M. (2000). Designing software for economic information systems. Moscow: Finance and Statistics, 352 p. [In Russian].

L. S. Sikora[1], N. K. Lysa[1], O. M. Pavluk[1], V. I. Sabat[2], O. Yu. Fedevych[1]

[1] *Lviv Polytechnic National University, Lviv, Ukraine*
[2] *Ukrainian Academy of Printing, Lviv, Ukraine*

INFORMATION AND LOGICAL-COGNITIVE APPROACHES TO THE FORMATION OF CYBERSECURITY OF ECOTECHNOGENIC INFRASTRUCTURES OF THE REGION TAKING INTO ACCOUNT THE LEVEL OF RISKS

The modern analysis stage of dynamics and goals of whole-oriented hierarchical systems infrastructure functioning with corporate and other types of management shows that current crisis and emergency situations arise due to past design errors. Uncertainty and undefined clarity of goals, underestimation of resources, selection of unclear strategies and main goals under the influence of cognitive failures in decision-making conditions, insufficient qualification of personnel, failure to take into account external threats, inability to predict active events for a long period of time are studied. Determining the level of threats at the expense of a low level of management training, respectively, leads to the collapse of infrastructure (region, state and local systems). Complication of technologi-

cal processes due to the modernization of complex technological processes aggregates with a distributed spatial infrastructure requires the use of new control systems and computer and information network technologies for the data transmission and processing about the state of aggregates and objects. Accordingly, this poses the problem of revising the basic concepts of information-measuring systems building, developing software and hardware for the implementation of the target management process, and creating sensors based on new methods of data selection of problem situations. This requires the development of new approaches to presentation, processing, and display of data on the aggregates state of energy-active objects and the entire information structure. At the same time, it is necessary to take into account that both technological and management systems have a hierarchical structure. For management under threat conditions, it is necessary to consider the features of the information infrastructure, data selection and processing methods, methods and algorithms for classifying the situation, which are formed from blocks of data obtained from each unit and the technological process as a whole. Information on the current state of the system and the infrastructure is necessary for the formation, adoption, and implementation of management decisions. Appropriate target orientation, reasonable indicators of real trajectories divergence from the target state determine the probability of an attack. Knowledge and decision-making procedures for the coordination of managerial actions is based on the strategic target orientation of the structure, their professionalism and the level of intellectual, cognitive, and scientific training. Information necessary for decision-making on the operative personnel team management is formed from data of various types, which is perceived from multimedia panels from the information system of the ACS-TP (technological process automated control system), which are in the cognitive system attention field of each of them (as intelligent agents). Accordingly, methods of assessing the situation to detect failures and the actions of attacks have been developed for each level of the infrastructure hierarchy, oriented towards strategic goals in the global infrastructure dynamic environment based on which countermeasures are formed depending on the type of threats.

Keywords: cyber security; infrastructure; system; management; cognitive models; information technologies; strategies; risks; target orientation; energy activity; hierarchy.