Нестеренко Олександр Васильович
доктор технічних наук, доцент, старший дослідник,
дійсний член Міжнародної академії інформатики,
професор ВНЗ «Національна академія управління»,
Заслужений працівник сфери послуг України,
м. Київ, Україна

Нетесін Ігор Євгенійович
кандидат фізико-математичних наук,
провідний науковий співробітник ДП «УкрНЦРІТ»,
м. Київ, Україна

Поліщук Валерій Борисович
кандидат технічних наук,
директор ДП «УкрНЦРІТ»,
м. Київ, Україна

МЕТОДОЛОГІЯ АВТОМАТИЗАЦІЇ ПРОЦЕДУРИ ЕКСПЕРТНОГО ОЦІНЮВАННЯ СПРОМОЖНОСТЕЙ В ОБОРОННОМУ ПЛАНУВАННІ

У останні роки в Міністерстві оборони України та Збройних Силах України проводяться заходи щодо інтеграції у процес оборонного планування (*Defence Planning Process*) моделі оборонного планування на основі спроможностей (ОПОС) (*Capability-Based Defence Planning*), яка застосовується в країнах-членах НАТО [1]. ОПОС полягає у формуванні за визначених економічних умов комплексних оперативних спроможностей сил оборони щодо протидії загрозам для гарантованого виконання ними завдань за призначенням.

Планування здійснюється у складному інформаційно насиченому середовищі на основі варіантів застосування різних складових сил оборони для виконання завдань, визначених за прогнозованими сценаріями. При цьому в рамках ОПОС потрібно також забезпечити прийняття раціональних рішень щодо розвитку спроможностей військових сил і засобів виконувати певні завдання. Ця процедура включає низку заходів щодо оцінювання спроможностей та формування цільового пакету необхідних спроможностей (див. рис. 1). Тому вкрай важливим є надання військовим підрозділам достатньо простої і в той же час науково-обґрунтованої методики оцінювання спроможностей. Така методика має забезпечувати експертам оперативно здійснювати вибір спроможностей або інших складових оборонного планування за простою уніфікованою процедурою.

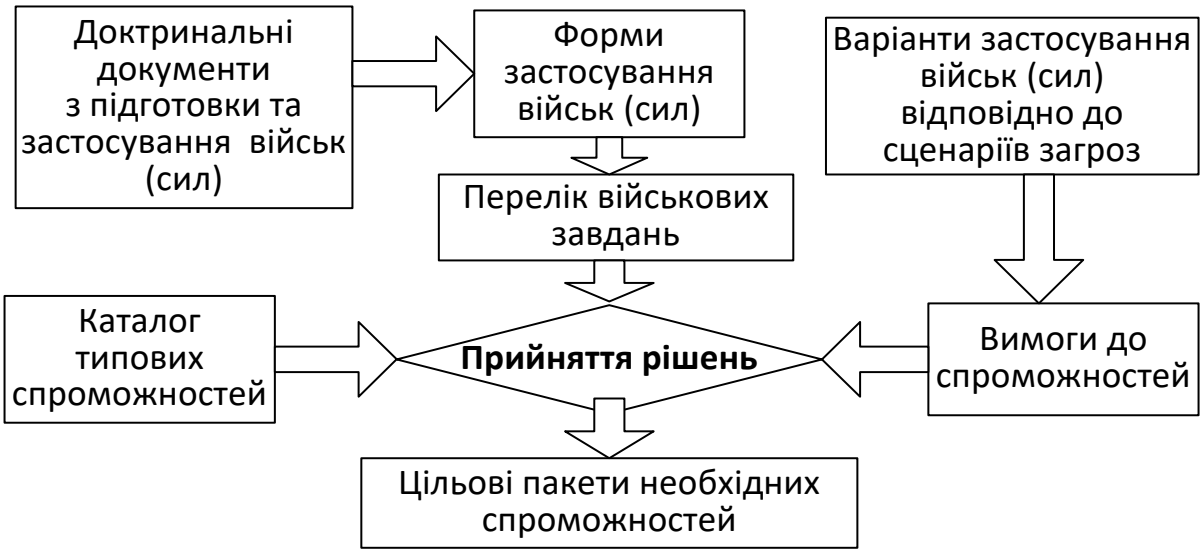

Рис. 1. Процедура формування цільового пакету необхідних спроможностей

Основною технологією процедури формування цільового пакету спроможностей є аналітична діяльність зі встановлення причинно-наслідкових зв'язків між різного роду даними та їхнє дослідження під всілякими кутами зору. Тому найважливішою умовою успішної аналітичної роботи експерта в органі військового управління (ОВУ) є наявність у його розпорядженні інформаційного поля досліджуваної предметної області (ПдО). Це поле представляє множину структурованих і неструктурованих інформаційних масивів (інформаційних ресурсів), потрібних для екстракції з них необхідних даних. Можливість експерту-аналітику керувати процесами обробки і аналізу таких даних можуть забезпечити лише засоби відповідної інформаційно-аналітичної системи (ІАС).

Діяльність в системі військового управління в умовах функціонування ІАС ґрунтується на моделях інформаційних потоків. На шляху цих потоків зазвичай існують певні бар'єри та перешкоди, інформаційні перенавантаження, втрачання інформації, що потребує управління потоками, яке базується на процесно-орієнтованому підході. Згідно зі стандартами НАТО систематику процесів та сервісів для ОВУ представляє поняття «бізнес-процес». Таким чином в умовах застосування ІАС побудова причинно-наслідкових ланцюжків у відповідності до бізнес-процесів дозволяє оброблені дані перетворити в нове знання та синтезувати відповідні рекомендації для осіб, що приймають рішення [2].

На якість підготовленого рішення впливає складність відображання і сприйняття експертом властивостей та функціональності складових об'єктів та процесів ПдО, тому об'єктні представлення предметних областей та описи конкретних процесів, що базуються на певних судженнях і твердженнях, мають бути задані відповідними інформаційними моделями, які з певним рівнем деталізації можуть бути подані ієрархічними структурами. Одним з інструментів, який може забезпечити відображення взаємодії усіх

інформаційних компонентів та допомогти достатньо ефективно спроектувати та реалізувати механізми управління ієрархією компонентів є онтологічна модель [3, 4].

Ієрархії, в яких відображаються властивості інформаційних процесів і ресурсів, дозволяють застосовувати експертні методи багатокритеріального вибору альтернатив, серед яких для ранжування спроможностей за певними критеріями в багатьох роботах, наприклад, в [5] пропонується застосувати метод аналізу ієрархій (MAI). Водночас треба зауважити, що MAI не позбавлений певних недоліків, зокрема щодо чутливості до чіткості визначення переліку альтернатив та обмежень, а також щодо відношень узгодженості як показників якості експертних оцінок. Тому для подолання вищезазначених недоліків пропонується вдосконалити MAI шляхом застосування методу схвального голосування експертів на етапі визначення переліку альтернатив, а також візуалізацією процесу парного порівняння альтернатив на основі ациклічних орієнтованих графів із застосуванням процедури транзитивного замкнення з автоматичним контролем узгодженості суджень експертів. Такий підхід до вирішення проблеми виходить із природної схильності людей оперувати візуальними образами та їх здатністю не тільки порівнювати об’єкти/властивості, а й оцінювати інтенсивність переваги.

Подібні підходи дозволяють знаходити найбільш прийнятні рішення у випадках, коли стан ПдО чітко відомий із заданим ступенем точності, а його формалізований опис поданий у вигляді визначених множин концептів та їх властивостей. Ця частина проблеми може бути вирішеною шляхом поєднання формалізації ПдО та структурування інформації, що базується на онтологічній моделі, з фреймовими структурами [6]. Фрейм містить на підставі семантичних ознак порожні рольові позиції (слоти), які після заповнення конкретними даними перетворюють фрейм у носій конкретного знання про предметну область з можливістю навігації контентом.

Сукупність запропонованих методів та підходів апробовано в системі автоматизованого супроводу розв’язання експертних задач на модельному прикладі оцінювання спроможностей для забезпечення ведення розвідки в інтересах наземної артилерії. Реалізована методологія дозволяє віднести вказану систему до категорії інтелектуальних систем.

Список використаних джерел

1. Оборонна реформа: системний підхід до оборонного менеджменту: монографія / А. Павліковський та ін. За заг. ред. д. військ. н. А. Сиротенка. Київ: НУОУ, 2020. 274 с.

2. Поліщук В.Б., Нетесін І.Є., Нестеренко О.В. Інформаційні технології в управлінні обороннимі ресурсами: методологічний контекст та приклади практичної реалізації. Частина 1: Монографія / За ред. В.Б. Поліщука. Київ: УкрНЦ РІТ, 2019. 120 с.

3. Gruninger M. Ontologies to support process integration in enterprise engineering / M. Gruninger, K. Atefi, M. Fox // Computational and Mathematical Organization Theory. 2000. Issue 6. P. 381-394.

4. Nesterenko O., Trofymchuk O. Patterns in forming the ontology-based environment of information-analytical activity in administrative management. Eastern-European Journal of Enterprise Technologies, 2019, № 5/2 (101). P. 33-42. DOI: 10.15587/1729-4061.2019.180107

5. Oleksandr Nesterenko, Igor Netesin, Valery Polischuk, Oleksandr Trofymchuk. Development of a procedure for expert estimation of capabilities in defense planning under multicriterial conditions. Eastern-European Journal of Enterprise Technologies. 2020. № 4/2 (106). P. 33-43. DOI: 10.15587/1729-4061.2020.208603.

6. Литвин В.В. Бази знань інтелектуальних систем підтримки прийняття рішень. Львів: Видавництво Львівської політехніки, 2011. 240 с.

Самарець Георгій Іванович
кандидат політичних наук
Воєнно-дипломатична академія імені Євгенія Березняка

Марилів Олександр Олександрович
кандидат технічних наук
Воєнно-дипломатична академія імені Євгенія Березняка
м. Київ, Україна

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ TLSI ДЛЯ КІБЕРЗАХИСТУ ОБ'ЄКТІВ НАЦІОНАЛЬНОГО ГОСПОДАРСТВА

З початком російської військової агресії у 2014 році кількість загроз у кіберпросторі України невпинно збільшується. Методи проведення кібератак на державні та приватні об'єкти господарства постійно вдосконалюються. Як наслідок, держава зазнає значних матеріальних збитків, що викликане втратою або спотворенням стратегічно важливої інформації. Однією з цілей проведених кібератак було виведення з ладу енергетичної системи в окремих районах України. Кібератак зазнали комп'ютерні системи управління трьох енергопостачальних компаній на заході України. Загалом, було вимкнено близько 30 електропідстанцій, 230 тисяч мешканців Прикарпаття залишались без світла протягом шести годин. Для кібератаки використовувалась троянська програма «Black Energy». Таким чином, кібератаки на об'єкти національного господарства можуть призвести до різних негативних наслідків, наприклад: техногенні катастрофи, фінансові збитки, виведення з ладу критичної і військової інфраструктури держави тощо [1].

Нажаль, Україна на даний час все ще залишається полігоном сучасних кібервійни та платить високу ціну за ігнорування питаннями безпеки кіберпростору. Таким чином, питання удосконалення методів ведення кібероборони, впровадження новітніх технологій кіберзахисту та їх постійне вдосконалення є актуальним напрямом наукових досліджень в даній області.

Для захисту інформації (державної, корпоративної або особистої) адміністратори мережевої безпеки використовують політику шифрування мережевого трафіку в середині локальної мережі та за її межами. Проте і