УДК 004.056:159.95

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 4, pp. 342-352

МЕТОД МОДЕЛЮВАННЯ ДІЯЛЬНОСТІ СУБ'ЄКТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З ВИКОРИСТАННЯМ ОПЕРАТОРІВ, ЩО ДІЮТЬ В ОНТОЛОГІЯХ ПРЕДМЕТНИХ ОБЛАСТЕЙ

А.А. Шиян

Вінницький національний технічний університет,
вул. Хмельницьке шосе, 95, Вінниця, 21021, Україна; e-mail: aa_shiyan@mail.ru

В статті розроблено математичний апарат та метод моделювання діяльності суб'єктів інформаційної безпеки, який базується на використанні множини операторів, що діють в спеціальним чином структурованих онтологіях предметних областей, навантажених ціллю. Доведено, що довільний оператор можна звести до певної сукупності двокомпонентних операторів, дія яких зв'язує дві компоненти онтології, одну до, а другу після здійснення діяльності. Наведено ряд прикладів застосування розробленого методу до моделювання суб'єктів інформаційної безпеки.

Ключові слова: інформаційна безпека, метод, онтологія, діяльність, предметна область, суб'єкт

Вступ

Інформаційна безпека – це захищеність інформації та інфраструктури, яка її підтримує, від випадкових або навмисних впливів природного чи штучного характеру, які можуть завдати неприйнятної шкоди суб'єктам інформаційних відносин, у тому числі власникам і користувачам інформації та підтримуючій інфраструктурі [1]. В [1, 2] показано, що сьогодні існує велика кількість визначень терміну «інформація», – але всі вони включають в себе, явно чи неявно, те, що тільки *суб'єкт* може як створити, так і користуватися інформацією.

Для суб'єкта характерно, що він має *внутрішні* степені свободи, які й надають йому можливість займати *активну* позицію в інформаційних відносинах. Проявляється це, наприклад, через постановку цілей, вибору однієї/декількох із множини можливих альтернатив, прояв індивідуальних переваг суб'єкта тощо.

На сьогодні в якості суб'єкту можуть виступати тільки люди, - окрема людина, їх структуровані чи неструктуровані об'єднання, суспільні інститути, суспільство в цілому та держава.

Таким чином, дослідження ролі суб'єктів в інформаційних відносинах, аналіз їх характеристик в різних умовах є важливим напрямком наукових досліджень у сфері інформаційної безпеки та її практичних застосувань.

Аналіз літератури та постановка задачі.

Існує багато підходів до опису основного суб'єкту інформаційної безпеки – людини [1, 2]. Умовно їх можна розділити на два великих класи. До першого можна віднести опис суб'єкта в рамках переважно психологічних перемінних [2]. Другий

підхід базується на використанні характеристик суб'єкту, які описують його діяльність [1]. Слід відмітити, що для практичних потреб використовують, як правило, змішані підходи, які описують і психологічні, і діяльні класи.

В [3, 4] розроблено підхід до опису суб'єкта діяльності, який використовує спеціальним чином структурований інформаційний простір задачі. Для цього вся сукупність даних розбивається спеціальним чином, *універсальним* для кожної задачі, на вісім класів (1), які не перетинаються між собою.

$$I_b = \sum_k \oplus I_b^k, \quad \forall k, m : I_k \cap I_m = 0, \tag{1}$$

де

I_b — інформаційний простір задачі *до* здійснення діяльності,

I_b^k — k-та компонента відповідного інформаційного простору,

$k = 1,...,8$ — нумерація компонент інформаційного простору задачі.

Індексами b та a позначаються інформаційні простори задачі *до* та *після* здійснення діяльності людиною.

Схематично метод розбиття множини даних (характеристик) про предметну область онтології на класи-компоненти (тобто алгоритм виділення компонент інформації із даного загального опису) [3, 4] можна представити таблицею 1.

Таблиця 1.

Опис компонент онтології (як інформаційного простору задачі для заданої цілі)

Дані про предметну область онтології	дані про клас подібних об'єктів (узагальнюючі компоненти інформації)	опорні елементи класу (структура, топологія)	Статичність, незмінність	Ст-С
			Динамічність, мінливість	Ст-Д
		границя між даним класом і іншими	Статичність, незмінність	Гр-С
			Динамічність, мінливість	Гр-Д
	дані про саме цей об'єкт (деталізуючі компоненти інформації)	сам об'єкт як одиничний і унікальний	Статичність, незмінність	Об-С
			Динамічність, мінливість	Об-Д
		зв'язки цього об'єкту з іншими конкретними, подібними до нього	Статичність, незмінність	Зв-С
			Динамічність, мінливість	Зв-Д

Можна показати, що побудований за алгоритмом табл. 1 інформаційний простір задачі є онтологією [5]. Але, на відміну від існуючого підходу до визначення онтологій, інформаційний простір є такою онтологію предметної області, яка відповідає *конкретній та фіксованій* цілі діяльності. Такі онтології будемо називати онтологіями, навантаженими ціллю.

Із використанням онтологій предметних областей, навантажених ціллю діяльності, наявність діяльності визначається за досить простим алгоритмом. Спочатку будуємо онтології (інформаційні простори) I_b перед та I_a після здійснення суб'єктом діяльності. Якщо після діяльності спостерігаються зміни в компонентах інформації, які

становлять базис онтології (інформаційного простору), – то вважається, що діяльність над розглянутою системою була здійснена.

Застосування такого підходу до задач інформаційної безпеки дозволяє використовувати лише об'єктивні характеристики та параметри. Важливою перевагою є те, що при цьому в рамках єдиного методу описувати діяльність всіх суб'єктів інформаційної безпеки – і окремих людей, і їх об'єднань: підприємств, суспільних інститутів, суспільства та держави.

Метою статті є розробка методів моделювання діяльності суб'єктів інформаційної безпеки з використанням множини операторів, що діють в онтологіях предметних областей.

Основна частина

Спочатку опишемо математичний апарат, який буде застосовано до опису задач інформаційної безпеки.

В подальшому викладі терміни «інтер'єр» або «інтер'єр діяльності» будуть розглядатися як тотожні терміну «предметна область діяльності».

Визначення 1. Перетворення (зміну) *наповнення* базових компонент онтології (інформаційного простору) будемо називати *діяльністю*.

Розглянемо об'єкт, який здатний здійснити управління в сенсі, описаному вище. Для нього можна дати таке визначення:

Визначення 2. Об'єкт, який сприймає наповнення компонент онтологій, і який здатний трансформувати (змінювати, перетворювати) наповнення компонент онтологій, називається *абстрактним інформаційним автоматом (АІА)*.

Зауваження. Підкреслимо, що АІА оперує, у загальному випадку, двома *різними* онтологіями, навантаженими *однієї й тою ж самою* ціллю діяльності (інформаційними просторами задачі). Першу онтологію він «будує» *перед* прийняттям рішення, і вона для нього *програмуючу роль*. Другу онтологію АІА будує вже *після* здійснення діяльності (наприклад, управляючого впливу), і служить вона для того, щоб визначити, чи досягнута ціль діяльності.

В наведеному визначенні явно виділена здатність АІА до зміни наповнення компонент онтології, – наприклад, до зміни станів і/або процесів у системі. Фактично, АІА розглядається як окремий самостійний об'єкт (певна окрема система), який здатний, у відповідь на вплив зовнішніх чинників, відповідним чином змінювати деякі характеристики зовнішнього по відношенню до себе середовища.

Остаточно, АІА може розглядатися як об'єкт, який має таку структурну будову:

$$< input \mid output > . \qquad (2)$$

Сконструйовані в такий спосіб АІА своїм першим блоком сприймають (засвоюють) наповнення певних компонент онтологій та трансформують їх у компоненти онтологій (загалом кажучи – інші), в рамках яких і можна описати діяльність цього АІА (його «творчість», «керування», управління»). Іншими словами АІА, який побудовано відповідно до такого правила, може розглядатися як об'єкт, який реалізує набір методів (алгоритмів, режимів, способів, технологій) для здійснення діяльності.

Введений вище АІА може розглядатися як оператор, який діє в просторі онтологій предметних областей, навантажених *фіксованою* ціллю.

Для цього, користуючись побудованим базисом онтології, можна записати довільну інформацію про предметну область (інтер'єр) діяльності в такому вигляді

$$I = \sum_{k=1}^{8} I_k \cdot \vec{i}_k , \qquad (3)$$

де

i_k — базисні вектори простору компонент інформації (вони задають просто назви компонент онтології),

I_k — характеристики, які можуть бути віднесені до даної компоненти онтології (тобто наповнення цих компонент інформацією).

Таким чином, співвідношення (3) розуміється в тому сенсі, що I_k являє собою базу даних, яка відноситься до певного заданого класу інформації, яка описує саме цю компоненту онтології діяльності для розглядуваної нами задачі. В цьому сенсі «точка» в онтологічному просторі є сукупністю баз даних, які не перетинаються між собою, і кожна із яких відноситься тільки і тільки до однієї компоненти інформації, – див. (1).

Відмітимо, що I_k не є числом, внаслідок чого операція «покомпонентного додавання» повинна бути визначена як об'єднання двох однорідних (тобто таких, які описують ту ж саму компоненту онтології) баз даних в одну (наприклад, в рамках реляційної моделі даних). «Покомпонентне віднімання» визначається аналогічно. Операція множення на число, яка необхідна для завершення побудови лінійного простору, відповідає зміні масштабу для одиниць вимірювання при описі даних (відмітимо, що в її наявності немає необхідності, і в подальшому вона не використовується). В цьому сенсі запис (3) являє собою певне узагальнення лінійного простору. Підкреслимо, метрика в інформаційному просторі не вводиться, тобто «відстань» між точками в нашому підході не визначається.

Таким чином, діяльність може бути представлена у вигляді оператора G, який перетворює онтологію I_{before}, яка була побудована (задана) перед здійсненням акту діяльності, в онтологію I_{after} для цього ж інтер'єру діяльності, але яка побудована вже після здійснення акту діяльності. Сказане можна записати в такий спосіб:

$$I_{after} = G \cdot I_{before} . \qquad (4)$$

Неважко побачити, що визначений таким чином оператор G має таку властивість: якщо онтологія (інформаційний простір) розбивається на два підпростори I_{b1} і I_{b2}, які не перетинаються, то $G(I_{b1} + I_{b2}) = G(I_{b1}) + G(I_{b2})$. Ця властивість є наслідком тієї обставини, що розв'язання сукупності задач, кожна із яких отримується шляхом декомпозиції основної (складної) задачі на взаємодоповнюючі частини, кожна із яких розв'язується окремо, є рівнозначною розв'язанню початкової складної задачі. Звичайно, це виконано у випадку, коли ефекти синергії та нелінійності відсутні. Але це, власне, й означає, що підпростори I_{b1} і I_{b2} онтології не перетинаються (тобто не мають спільних точок).

Таким чином, якщо інформаційний простір I_{before} розбивається на пряму суму підпросторів (1), то внаслідок цього оператор G діє в такий спосіб:

$$I_a = \sum_k \oplus I_a^k = G\left(\sum_k \oplus I_b^k \right) = \sum_k \oplus G\left(I_b^k\right). \qquad (5)$$

У загальному вигляді із (5) випливає, що оператор G може бути представлений як тензорний оператор, у якого є n «нижніх» і m «верхніх» індексів. При цьому, в силу

наявності в онтології базису із восьма компонент, кількість як «верхніх», так і «нижніх» компонентів у тензора G_n^m обмежена 8: $n, m \le 8$.

Умовимося для простоти запису, що «нижні» компоненти відповідають компонентам інформації для інформаційного простору I_{before}, а «верхні» – відповідно для I_{after}.

Застосовуючи «умову Ейнштейна» про те, що за повторюваним індексах здійснюється сумація, (4) може бути переписане у такому вигляді.

$$I_a^{k1,k2,\dots} = G_{s1,s2,\dots}^{k1,k2,\dots} \cdot I_b^{s1,s2,\dots}. \qquad (6)$$

Використовуючи властивість (1) і (5), приходимо до висновку, що дія будь-якого тензорного оператора G_n^m виражається через дію суми $\max\{n, m\}$ квазілінійних операторів, які мають вигляд g_k^i.

Це твердження може бути сформульоване у вигляді такої теореми.

Теорема 1. Для здійснення будь-якої діяльності необхідно та достатньо наявності тільки таких AIA, які програмуються всього однією компонентою онтології I_{before} і діяльність яких виражається також у зміні всього однієї компоненти із онтології I_{after} (тобто результуюча зміна при переході від I_{before} до I_{after} полягає в зміні в онтології I_{after} всього однієї компоненти в порівнянні із онтологією I_{before}).

Доведення. Справедливість цієї теореми ґрунтується на тій обставині, що онтологія являє собою повний простір даних (відомостей, характеристик, параметрів тощо), які відносяться до розглянутої нами задачі.

У цьому сенсі будь-який оператор AIA: $I_{before} \to I_{after}$ діє як автоморфізм, тобто, по суті, не змінює нашої онтології: змінюється тільки «наповненість» її координат, тобто чисельні (або інші) значення її компонент. Для інших «двокомпонентних» AIA результат дії «попереднього» AIA є програмуючою онтологією. Ланцюжок можна продовжувати доти, поки це необхідно.

Достатність теореми випливає із тієї обставини, що, порівнюючи тільки «початкову» і «кінцевий» онтології між собою, ми не зможемо визначити, чи було управління здійснене оператором G_n^m, чи воно було здійснено сукупністю послідовно застосованих «двокомпонентних» операторів g_k^i. •

Символом «•» буде в статті позначатися закінчення доведення чи прикладу.

Іншими словами, ми можемо «замінити» одне управління, яке ґрунтується на сукупності компонент із онтології на суму послідовно застосовуваних актів діяльності, кожен із яких «задіює» усього одну компоненту із онтології I_{before} і результат застосування якого виражаємося в зміні всього однієї компоненти із онтології I_{after}. Це «майже очевидне» твердження являє собою, по суті, стандартний метод «розбиття» складної задачі на послідовні етапи. Як правило, досить часто таке розбиття на послідовні етапи здійснюється суб'єктом діяльності «навіть не замислюючись», як «очевидне».

Таким чином, в силу теореми 1, кожен оператор, який відповідає AIA, може бути виражений як сума певних «бінарних» операторів, що зв'язують між собою всього дві компоненти онтології: одну із простору I_{before}, а іншу – із простору I_{after}. Математично це можна записати таким чином.

$$g_{(n)}^{(m)} = \sum_{k=1}^{\max(n,m)} g_{(k)_i}^{\ j} . \qquad (7)$$

Неважко побачити, що для введених операторів g_k^i будуть справедливі такі теореми.

Теорема 2. Оператор g_k^i має властивість бути комутативним $g_k^i + g_p^l = g_p^l + g_k^i$ та асоціативним $g_1 + (g_2 + g_3) = (g_1 + g_2) + g_3$.

Доведення випливає із властивостей операторів g_k^i.

Теорема 3. Загальна кількість операторів g_k^i становить 64 різних варіантів.

Доведення. Бінарний оператор g_k^i може мати лише одну із восьми компонент з інформаційного простору I_{before} і лише одну із восьми компонент із інформаційного простору I_{after}. Кількість різних можливих варіантів становить 8×8=64. •

Наведемо ряд прикладів, які описують застосування операторів g_k^i для опису діяльності, включаючи діяльність в сфері розв'язання задач інформаційної безпеки. Відмітимо, що наведений вище метод моделювання діяльності, в його *практичному* застосуванні, відповідає переліку спеціальним чином структурованих *функціональних обов'язків*, які повинен виконувати суб'єкт діяльності.

Приклад 1. Розглянемо відцентровий (рос. центробежный) регулятор, прикладом якого є регулятор Уатта. З точки зору введених вище АІА він являє собою управління, яке влаштоване за таким алгоритмом.

$$< процес \mid стан > \qquad (8)$$

Звичайно, при цьому розглядається цілком певна характеристика об'єкту, який підлягає управлінню. Регулятор відслідковує певну характеристику об'єкту, після чого здійснює свою діяльність таким чином, щоб досягти її незмінності – тобто щоб досягти певного стану (заданого для цієї характеристики). •

Приклад 2. Іншим прикладом слугує регулятор, який не допускає, наприклад, флаттер (сукупність самозбуджених незатухаючих крутильних та згинальних коливань конструкцій літака, що призводять до його руйнування). В цьому випадку АІА, який здійснює діяльність, влаштовано «навпаки».

$$< стан \mid процес > \qquad (9)$$

В цьому випадку також розглядається цілком певна характеристика об'єкту, який підлягає управлінню.

Регулятор (9) відслідковує набір цілком *значень* (тобто *станів*) певних характеристик об'єкту, що управляється. А його діяльність полягає в започаткуванні *процесів*, які направлені на *зміну* «критичних» для об'єкту значень тих же самих характеристик.

Цікаво, що за аналогічним алгоритмом (9) також можна описати цілий клас регуляторів, які мають своєю ціллю недопущення параметричного резонансу елементів конструкції об'єкту (наприклад, які відповідають так званим «язикам Арнольда»). •

Підкреслимо, що в прикладах 1 та 2 розглядалися такі АІА, для яких інші полюси дихотомій компонент інформаційного простору є *однаковими*.

Приклад 3. В загальному вигляді *негативний* зворотній зв'язок задається виразом (8). Але, на відміну від попередніх прикладів, в ньому вже можуть використовуватися *декілька* компонент інформаційного простору задачі. •

Приклад 4. Позитивний зв'язок задається виразом (9), де теж, в загальному випадку, можуть використовуватися декілька компонент інформаційного простору задачі. •

Як видно із прикладів 3 та 4, велика частина стандартних задач загальної теорії управління та кібернетики в цілому допускає використання концепції АІА в якості стандартизованих елементів.

Але предметна область застосування АІА значно ширша, аніж теорія управління та кібернетика. Наведемо приклад, коли АІА можуть бути використані в якості аналога «природної мови» для побудови інтелектуальних систем в інформаційних технологіях.

Розглянемо спеціальний клас АІА – двокомпонентні АІА (скорочено 2АІА), кількість яких є *меншою* за 64, але які дозволяють описати будь-яку діяльність. Дамо для них таке визначення (назви базисних компонент інформації наведено в табл. 1).

Визначення 3. АІА називається двохкомпонентним (2АІА), якщо він задовольняє таким умовам:

1) Кожен 2АІА сприймає тільки одну компоненту інформації і здійснює діяльність теж тільки в рамках однієї компоненти інформації.

2) Для кожного 2АІА одна компонента описує статичність, а інша – динамічність.

3) Для кожного 2АІА одна компонента є узагальнюючою, а інша – деталізуючою.

Коректне визначення 2АІА саме як об'єкта, що реалізує ті або інші режими (типи, способи, алгоритми, методи, шляхи) діяльності, можливе тільки так, як описано вище.

Перша умова відповідає теоремі 1.

Друга умова також є необхідною. Дійсно, якщо допустити, наприклад, що 2АІА і програмуються процесом, і творять також процес, то також не одержимо оптимальної діяльності. По суті, тут також підійде принцип «бритви Оккама»: бо все рівно прийдеться вводити такі 2АІА, які мають вигляд <*стан* | *процес*> – так само як і <*процес* | *стан*>, бо тільки такі «додаткові» 2АІА можуть дозволити нам організувати «спілкування» у середовищі таких 2АІА. Наприклад, це необхідно для того, щоб «ставити завдання» перед такими АІА.

Нарешті, розглянемо третю умова. Припустимо, що ми визначили 2АІА таким чином, щоб одні з них реалізовували діяльність (тобто і програмувалися, і творили) тільки за деталізуючими компонентами, а інші тільки за узагальнюючими. У цьому випадку прийдеться вводити спеціальний новий тип 2АІА, який би «аналізував» ситуацію за допомогою узагальнюючих компонент онтології, – а роздавав би завдання вже для «деталізуючих типів 2АІА». Отже, третя умова також випливає із вимоги оптимальності для управління, реалізованого системою 2АІА («бритва Оккама»: не потрібно множити сутності без необхідності).

Відзначимо також, що при будь-якому іншому визначенні 2АІА їхня кількість буде більшою: отже, введений нами клас 2АІА є в цьому сенсі «мінімально необхідним».

Таким чином, 2АІА перетворює одну компоненту інформації (за допомогою своєї «сприймаючої функції») в іншу (за допомогою своєї «творчої, діяльнісної функції»).

Можна сказати, що,2АІА влаштовані так, що одна з їхніх компонент (будемо для неї також використовувати назву «функція») відповідає узагальненому опису предметної області, а друга її компонента відповідає конкретним одиничним об'єктам, із яких вона складається. Схематично це показано на рис. 1, де через Узаг і Дет позначені узагальнююча та деталізуюча компоненти інформації, відповідно. З рис. 1 видно, що клас 2АІА створює кільця зворотного зв'язку.

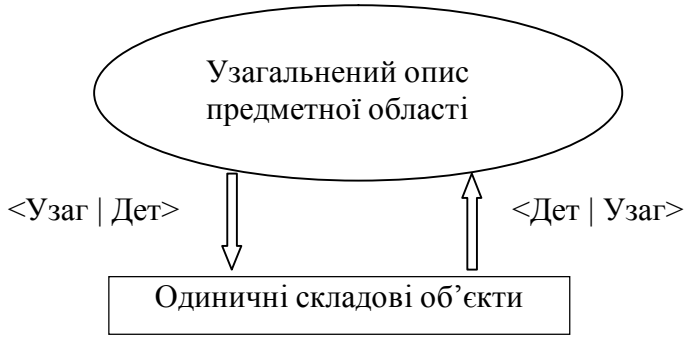

Рис. 1. 2AIA як об’єкти, що здійснюють перетворення компонент інформації в онтології предметної області

Підрахувати кількість різних типів 2AIA можна в такий спосіб. По-перше, у якості «вхідної» компонента може бути обрано будь-яку компоненту онтології. Значить – є вісім різних можливостей. А для другої потрібно відкинути ряд варіантів вибору для компонент онтології. Спочатку потрібно відкинути всі ті компоненти, які описують ту ж саму часову динаміку – тобто чотири компоненти онтології (наприклад, якщо вхідна компонента є статичною, то вихідна компонента інформації не може бути статичною). Далі повинні бути відкинуті компоненти онтології, які описують той же самий рівень, що і для вхідної компоненти онтології (наприклад, якщо вхідна компонента онтології є узагальнюючою – то вихідна компонента онтології узагальнюючої бути не може). Більше обмежень у визначенні 2AIA немає. В результаті залишаються 2 компоненти онтології, які можуть використаними в якості вихідної – за умови, коли вхідна компонента онтології є заданою. Наприклад, якщо вхідна компонента онтології є узагальнюючою та динамічною, то в якості вихідної можна взяти будь-яку компоненту із двох: статичну та деталізуючу (тобто або *Об-С* або *Зв-С*). Разом: вісім можливих варіантів входу помножити на два можливих варіанти виходу матимемо 16 різних типів 2AIA.

Таким чином, приходимо до такої теореми.

Теорема 4. Несуперечлива діяльність в загальному вигляді може бути здійснено сукупністю із 16-ти типів 2AIA, які мають наступний вигляд:

<Ст-С|Зв-Д>, <Ст-С|Об-Д>, <Ст-Д|Зв-С>, <Ст-Д|Об-С>,
<Гр-С|Зв-Д>, <Гр-С|Об-Д>, <Гр-Д|Зв-С>, <Гр-Д|Об-С>,
<Об-С|Ст-Д>, <Об-С|Гр-Д>, <Об-Д|Ст-С>, <Об-Д|Гр-С>,
<Зв-С|Ст-Д>, <Зв-С|Гр-Д>, <Зв-Д|Ст-С>, <Зв-Д|Гр-С>.

При записі типів 2AIA використані найменування компонент інформації, наведені в табл. 1. Перша компонента онтології відповідає входу в 2AIA, тобто опису тієї компоненти онтології, якою цей 2AIA програмується до дії (тобто яку він сприймає), а друга компонента – описує ту компоненту онтології, у рамках якої може бути виражена його діяльність. Нагадаємо, що ці компоненти онтології беруться в різні моменти часу.

Умови Теореми 1 і Теореми 4 приводять до такої теореми.

Теорема 5. Для здійснення довільної управлінської діяльності в довільній предметній області необхідно та достатньо наявності 16-ти типів 2AIA.

Іншими словами, для будь-якого інтер’єру реалізації як завгодно складної та витонченої діяльності необхідно та достатньо мати всього лише такі 16 типів 2AIA, які визначені вище.

Результат нашого розгляду вийшов досить нетривіальним: ми, по суті, побудували класифікацію всіх можливих типів діяльності. Теорема 5 говорить, що «інших типів» бути просто не може. Роз’яснимо це твердження більш докладно. Внаслідок Теореми 1 для здійснення довільно взятої діяльності в предметній області необхідно та достатньо мати набір тільки із *двокомпонентних* AIA. У відповідності із

Теоремою 4 несуперечливе управління можуть здійснювати тільки 16 спеціальним чином сконструйованих типів АІА, які ми позначили як 2АІА. Відмітимо, що в [6] доведено, що 2АІА є детермінованими скінченними автоматами.

В [4] доведено, що *раціональна* діяльність довільної людини повністю описується в рамках одного і тільки одного типу 2АІА.

Наведемо приклади застосування розробленого математичного апарату до задач інформаційної безпеки.

Розглянемо задачі забезпечення інформаційної безпеки держави. Суб'єктами інформаційної безпеки держави є суспільні та державні інститути та структури, угрупування людей, а також окремі індивіди. Опишемо приклади моделей діяльності деяких таких суб'єктів.

Приклад 5. Прокуратура як державний інститут повинна забезпечувати *виконання законів* в державі. Тобто результатом її діяльності повинен бути *стан*, а відслідковувати (програмуватися) вона повинна *відхиленнями* від цього стану, – тобто *процесом*. Таким чином, прокуратура повинна діяти в рамках *негативного* зворотного зв'язку, тобто в рамках формули (8). Більш того: закони формуються в рамках узагальнюючих компонент онтологій, тому програмуватися прокуратура повинна *узагальнюючими* компонентами, а результатом її діяльності є *деталізуючи* компоненти (наприклад, конкретні дії суб'єктів). Подальша деталізація компонент онтологій є неможливою: тут можуть бути різні варіанти. Таким чином, діяльність прокуратури може моделюватися як оператор G у вигляді $<Ст\text{-}Д,\ Гр\text{-}Д|Об\text{-}С,\ Зв\text{-}С>$, або відповідними чотирма відповідними типами 2АІА із теореми 5. Це означає, до речі, що діяльність прокуратури можна повністю звести до діяльності *окремих типів* 2АІА (наприклад, вона може бути здійснена конкретними людьми).

Використання прокуратури як державного інституту в рамках інших компонент онтологій предметної області законодавства буде суперечити її ролі, і приведе до зниження рівня інформаційної безпеки держави. •

Приклад 6. Інститут суду (юстиції) в державі повинен забезпечувати *рівновагу* в суспільстві. Це значить, що повинен програмуватися *станом* суспільства, а результатом його діяльності також повинен бути *стан* (той же, або *інший*). Таким чином, к вигляді оператора G діяльність судової системи записується у вигляді $<Стан|Стан>$.

Виконання такої діяльності неможливо забезпечити однією людиною, і тому в рамках судового процесу обов'язково повинні приймати участь *декілька* людей (звичайно, крім самого порушника закону, – втім, в рамках судового процесу він розглядається не як суб'єкт, а в якості об'єкту для застосування норм права). Власне, *інститут адвокатури* (а також інститут присяжних) виник саме в якості механізму, який призваний забезпечити *виконання діяльності* інститутом суду за допомогою *людей* (кожен із яких має конкретний тип 2АІА).

Так як, відповідно до прикладу 5, інститут прокуратури як учасник судового процесу може бути представлений у вигляді $<Процес|Стан>$, то діяльність інституту адвокатури повинна виглядати як $<Стан|Процес>$, тобто забезпечувати *позитивний* зворотний зв'язок. Таким чином, інститут суду дійсно *здатний забезпечити* встановлення рівноваги в результаті *змагальності* прокуратури та адвокатури.

Відмітимо, що судова система держави може бути використана за двома *різними* каналами. Перший визначається оператором G $<Стан|Стан>$, тобто діяльністю із *збереження* існуючого в суспільстві та державі стану. Цей канал відповідає континуальному (або кодексному) праву, характерному, в тому числі, і для України. Другий канал визначається оператором G, який має вигляд $<Стан\text{-}1|Стан\text{-}2>$, тобто за цих умов діяльність судової системи держави здатна *змінювати* існуючий у суспільстві та державі стан. Цей другий канал відповідає *прецедентній* правовій системі. Короткий історичний огляд формування та порівняння прецедентної та континентальної судових

систем як суспільних інститутів здійснено в [7], де доведено, що *адаптаційні* властивості кращі для прецедентного права. Підкреслено, що на етапі *трансформації* в суспільстві та державі, прецедент не право дозволяє різко *знизити* рівень суспільної напруженості та запобігти революційним виступам населення.

Цікаво, що в Україні Верховний Суд працює *частково* також і в рамках прецедентного права: ряд його рішень можуть бути використані судами нижчої інстанції в якості прецедентів. •

Приклад 7. Законодавча та виконавська системи влади в країні виконують діяльність в рамках оператора G, який має вигляд $<Узаг|Дет>$: вони, виходячи із «інтересів держави», здійснюють діяльність з управління конкретними об'єктами та суб'єктами держави.

Отже, із «трьох гілок влади» в держави дві гілки працюють в одному напрямку: від інтересів держави, якій вони підпорядковують інтереси суб'єктів більш низького рівня ієрархії (підприємств, суспільних груп та окремих індивідів). Судова влада в рамках контингентного права також підпорядковує інтереси громадян інтересам держави.

Таким чином, в ряді держав (в тому числі і в Україні) спостерігається явне домінування держави практично у всіх сторонах життя людей.

Для забезпечення потрібного рівня інформаційної безпеки держави необхідно, щоб в ній цей «перекіс» урівноважувався суспільними інститутами, діяльність яких описується в рамках оператора G $<Дет|Узаг>$. Діяльність цих інститутів полягає в *інформуванні* гілок державної влади щодо явищ та реалій суспільного життя. Фактично, тільки за їх наявності формується *кільце* зворотного зв'язку, яке показано на рис. 1.

Саме таку інформаційну будову мають ЗМІ та громадські організації (включаючи політичні партії). Саме тому в *розвинених* країнах велика увага приділяється тому, щоб ці суспільні інститути були *незалежні* від держави. •

Таким чином, розроблений математичний апарат можна використовувати для аналізу широкого кола задач інформаційної безпеки держави, притому як на макрорівні, так і на рівні забезпечення інформаційно-психологічної безпеки людини, суспільства та держави. При цьому виникає можливість конструювати інформаційні системи, які складаються із суб'єктів інформаційної безпеки, з використанням фрагментів, які описуються відповідними АІА та 2АІА.

Висновки

В статті розроблено математичний апарат та метод моделювання діяльності суб'єктів інформаційної безпеки. Метод моделювання базується на використанні множини операторів, що діють в спеціальним чином структурованих онтологіях предметних областей, навантажених ціллю. Доведено, що довільний оператор можна звести до двокомпонентного, дія якого зв'язує дві компоненти онтології, одну до, а другу після здійснення діяльності. Побудовано множину із мінімальної кількості двокомпонентних абстрактних інформаційних автоматів (2АІА). Наведено ряд прикладів застосування розробленого методу моделювання до опису суб'єктів інформаційної безпеки.

Список літератури

1. Андреєв, В.І. Основи інформаційної безпеки: підручник / В.І. Андреєв, В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест; Держ. ун-т інформ.-комунікац. технологій. — 2-ге вид., доповн. і переробл. — К., 2009. — 293 с.

2. Манойло, А.В. Государственная информационная политика в особых условиях [Текст] : монография / А.В. Манойло. — М. : МИФИ, 2003. — 388 с.
3. Шиян, А. А. Информационное пространство и классификация стратегий управленческой деятельности в теории игр и принятия решений / А.А. Шиян // Інформаційні технології та комп'ютерна інженерія. — 2007. — № 3(10). — С. 131–139.
4. Шиян, А.А. Теоретико-ігровий аналіз раціональної поведінки людини та прийняття рішень в управлінні соціально-економічними системами [Текст] : монографія / А.А. Шиян ; Вінниц. нац. техн. ун-т. — Вінниця : Універсум - Вінниця, 2009. — 404 с.
5. Handbook on Ontologies: International Handbooks on Information Systems / Eds. S. Staab and R. Studer. — 2nd edition. — Berlin : Springer, 2009. — 832 p.
6. Шиян, А.А. Механізм та технології для управління колективом на основі моделі детермінованих скінченних автоматів / А.А. Шиян, Л.О. Нікіфорова, Т.К. Мещерякова // Вісник Хмельницького національного університету. Економічні науки. — 2012. — № 2, Т. 1. — С. 46–49.
7. Шиян, А.А. Управління формуванням ефективних економічних інститутів в умовах України [Текст] : монографія / А.А. Шиян, Л.О. Нікіфорова ; Вінниц. нац. техн. ун-т. — Вінниця : ВНТУ, 2011. — 300 с.

МЕТОД МОДЕЛИРОВАНИЯ ДЕЯТЕЛЬНОСТИ СУБЪЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ ОПЕРАТОРОВ, ДЕЙСТВУЮЩИХ В ОНТОЛОГИЯХ ПРЕДМЕТНЫХ ОБЛАСТЕЙ

А.А. Шиян

Винницкий национальный технический университет,
ул. Хмельницкое шоссе, 95, Винница, 21021, Украина; e-mail: aa_shiyan@mail.ru

В статье разработан математический аппарат и метод моделирования деятельности субъектов информационной безопасности, который базируется на использовании множества операторов, действующих в специальным образом структурированных онтологиях предметных областей, которые нагружены целью. Доказано, что произвольный оператор можно свести к определенной совокупности двокомпонентных операторов, действие которых связывает две компоненты онтологии, одну до, а вторую после осуществления деятельности. Описан ряд примеров применения разработанного метода к моделированию деятельности субъектов информационной безопасности.

Ключевые слова: информационная безопасность, метод, онтология, деятельность, предметная область, субъект

A TECHNIQUE TO MODEL THE ACTIVITIES OF INFORMATION SECURITY SUBJECTS INVOLVING THE APPLICATION OF OPERATORS ACTING IN DOMAIN ONTOLOGIES

Anatoliy A. Shiyan

Vinnytsia National Technical University,
95 Khmelnytske shose, Vinnytsia, 21021, Ukraine; e-mail: aa_shiyan@mail.ru

In this work, a mathematical apparatus for, and a technique to model, information security subjects were developed based on application of operators acting in specially-structured domain ontologies loaded with a target. It was proved, that an arbitrary operator can be reduced to a definite collection of two-component operators, with the action of the latter binding the first and second components of onthology before and after performance of the activity, respectively. Several examples of application of the technique developed to model the activity of information security subjects were given.

Keywords: information security, method, ontology, activity, subject area, subject