УДК 004.415.056.5(075)

ПОНЯТТЯ КЛАСИФІКАТОРУ І ТОПОСІВ У ПІДОБ'ЄКТАХ МНОЖИН СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Павлов І.М.

CONCEPT CLASSIFIER AND TOPOS IN UNDER OBJECTS SETS OF INFORMATION SECURITY

Pavlov I.

У статті розглядається категорний аналіз взаємовідносин множин та підмножин з метою проведення просторового аналізу загрозливих впливів на системи захисту інформації.

Ключові слова: *множина, підмножина, об'єкти, підоб'єкти, система захисту інформації, топоси, функції.*

Вступ

На сьогоднішній момент створення систем захисту інформації (СЗІ) не можливе без дослідження й узагальнення світового досвіду побудови інформаційних систем та їх складових підсистем, одними з ключових яких є системи захисту інформації. Математичним забезпеченням таких систем є моделі процесів нападу на механізми захисту та блокування або знищення самих загроз. Базою таких моделей є математичний апарат, який повинен забезпечити адекватність моделювання процесів захисту інформації для будь-яких умов впливу загроз [1-3].

Постановка проблеми

При визначенні математичного апарату необхідно чітко розуміти як будуються ті або інші множини загроз, та як здійснюється взаємовідносини самих множин загроз та множин механізмів захисту, їх бар'єрів. У статті пропонується математичний апарат теорії топосів, який дозволяє на рівні категорійного апарату логіки моделювати побудову множин у просторовому часі, пропонуючи конкретні математичні категорії та моделі для опису таких взаємовідносин. *Тому метою цієї статті є* подальше визначення математичного апарату побудови моделей взаємовідносин уразливих множин загроз та множин систем захисту інформації.

Основна частина

Функція $f: A \to B$ з множини A у множині B стає елементом множини B^A, тобто $f \in B^A$. Тому виникає функція $\ulcorner f \urcorner: \{0\} \to B^A$, така, що $\ulcorner f \urcorner(0) = f$. Якщо x – елемент з A, то мається категорійний елемент $\bar{x}: \{0\} \to A$, який визначається рівнянням $\bar{x}(0) = x$. Так як $\mathrm{ev}(\langle f, x\rangle) = f(x)$ [2], то $\mathrm{ev} \circ \langle \ulcorner f \urcorner, \bar{x}\rangle(0) = \mathrm{ev}\big(\ulcorner f \urcorner(0), \bar{x}(0)\big) = f(x) = f\big(\bar{x}(0)\big)$, і отримується рівняння функцій: $\mathrm{ev} \circ \langle \ulcorner f \urcorner, \bar{x}\rangle = f \circ \bar{x}$.

Ця ситуація може бути розповсюджена на вільну категорію, яка допускає експоненсування. Для β-стрілки $f: a \to b$ побудуємо стрілку $f \circ pr_a: 1 \times a \to b$ яка є композицією $f \circ pr_a: 1 \times a \to a \to b$. Тоді *іменем* f можна назвати стрілку $\ulcorner f \urcorner: 1 \to b^a$, яка є експоненціально приєднаною до стрілки $f \circ pr_a: 1 \times a \to b$. Таким чином, $\ulcorner f \urcorner$ – це єдина стрілка, для якої діаграма, наведена на рис. 1. є комутативною.

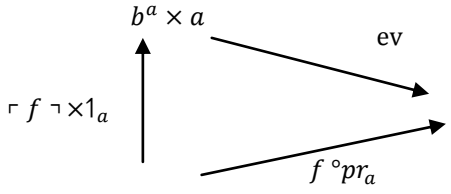


Рис. 1. Комутативна діаграма імені функції f

Для вільного β-елементу $x: 1 \to a$ об'єкта a мається рівняння $\mathrm{ev} \circ \langle \ulcorner f \urcorner, x\rangle = f \circ x$.

Розглянемо множини через декілька точок. У теорії множин [5] *множина-ступінь* $\mathcal{P}(D)$ позначається через 2^D при сукупності усіх функцій з D у $2 = \{0,1\}$ (рис. 2).

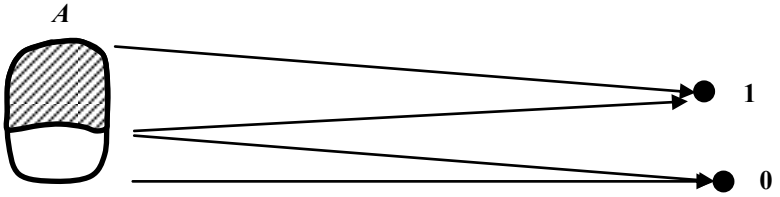


Рис. 2. Діаграма множини-ступені $\mathcal{P}(D)$

Основою для такого позначення є наявність ізоморфізма $\mathcal{P}(D) \cong 2^D$, тобто взаємно однозначної відповідності між підмножинами множини D і функціями $D \to 2$. Цей ізоморфізм встановлюється наступним чином. Для підмножини $A \subseteq D$ визначимо функцію $\chi_A: D \to 2$, яка має назву характеристичної функції множини A, правилом: для елементів з D, які належать A, значення цієї функції дорівнює 1, а для елементів, які не належать A, воно дорівнює 0, тобто:

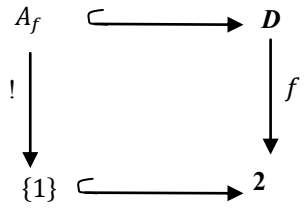
$$\chi_A(x) = \begin{cases} 1, \text{якщо } x \in A, \\ 0, \text{якщо } x \neq A. \end{cases} \quad (1)$$

Відображення, яке ставить у відповідність множині A функцію χ_A, є ін'єктивним відображенням з $\mathcal{P}(D)$ у 2^D, тобто якщо $\chi_A = \chi_B$, то $A = B$. Воно також сур'єктивно, тобто $f \in 2^D \implies f = \chi_{A_f}$, де $A_f = \{x: x \in D \text{ і } f(x) = 1\}$.

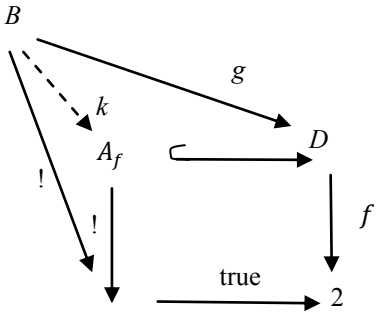
Ця відповідність між підмножинами і характеристичними функціями може бути викладена категорично за допомогою зворотного образу.

Множина A_f, яка визначена (5) є прообразом при відображенні f підмножини $\{1\}$ множини $\{0,1\}$, тобто: $A_f = f^{-1}(\{1\})$.

Діаграма у вигляді декартового квадрату представлена на рис. 3а.



а)

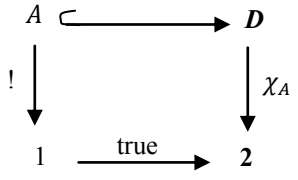


б)

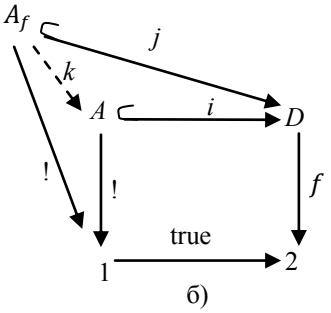
Рис. 3. а) Декартів квадрат множини $A_f = f^{-1}(\{1\})$.
б) Комутативна діаграма декартового квадрату

Тобто A_f отримується шляхом під'єму стрілки $\{1\} \hookrightarrow 2$ вдовж f. Якщо нижню стрілку замінити функцією з $1 = \{0\}$ у $2 - \{0,1\}$, яке приймає значення 1, то отримуємо функцію true (істина). Таким чином, $\text{true}(0) = 1$ і внутрішній квадрат діаграми, наведеної на рис. 3б є декартовим.

Дійсно, якщо уявити що зовнішній "квадрат" комутативний, тоді, якщо $b \in B$ і $f\big(g(b)\big) = \text{true}\big(!(b)\big) = 1$, то $g(b) \in A_f$. Тому при $k: B \to A_f$, яке визначено рівнянням $k(b) = g(b)$, уся діаграма буде комутативною, але при одному k. Відповідно, якщо $A \subseteq D$, то квадрат, представлений на рис. 4а. декартовий, так як під'єм true вдовж χ_A дає множину $\{x: \chi_A(x) = 1\}$, яка дорівнює A.



а)

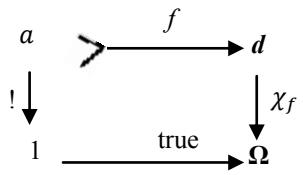


б)

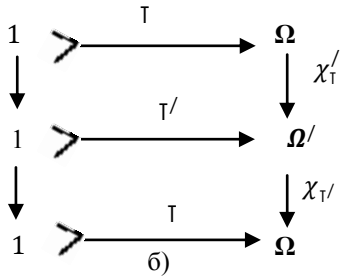
Рис. 4. а) Декартів квадрат множини $A \subseteq D$.
б) Комутативна діаграма декартового квадрату при $A \subseteq A_f$

Більш того, χ_A можна визначити як єдину функцію з *D* у 2, яка переводить приведену на рис. 5. діаграму у декартов квадрат, тобто як єдину функцію, під'єм вдовж якої функції true дає *A*. Дійсно, якщо для деякої функції f внутрішній квадрат у діаграмі (наведеної на рис. 4б) декартовий, то для $x \in A$ буде $f(x) = 1$, так що $x \in A_f$. Тому $A \subseteq A_f$.

Так як зовнішній "квадрат" комутативний, то існує єдина функція *k*, яка задовольняє рівнянню $i \circ k = j$. Оскільки функції *i* та *j* є включеннями, то *k* також повинна бути включенням. Таким чином, $A_f \subseteq A$ що сумісно з попереднім дає $A_f = A$, але f є характеристичною функцією множини A_f, тому $f = \chi_A$. У подальшому можна визначити наступну тезу. Якщо мається β-категорія з кінцевим об'єктом 1, то *класифікатором підоб'єктів* для β можна назвати β-об'єкт Ω сумісно з β-стрілкою $\text{true}: 1 \to \Omega$, такий, що виконується наступне твердження, що для кожної стрілки $f: a \to d$ існує одна і тільки одна β-стрілка $\chi_f: d \to \Omega$, для якої діаграма, яка наведена на рис. 5а є декартовим квадратом.



а)



б)

Рис. 5. а) Декартів квадрат множини β-стрілки $\chi_f: d \to \Omega$. б) Діаграма класифікаторів підоб'єктів $\top: 1 \to \Omega$ і $\top^{/}: 1 \to \Omega^{/}$

Також таку стрілку називають [5] *характером монострілки f* (підоб'єкту *d*). У подальшому стрілка true буде позначатися як T^1 .Для визначення класифікаторів піоб'єктів припустимо, що $T: 1 \to \Omega$ і $T^{/}: 1 \to \Omega^{/}$ є класифікаторами підоб'єктів. Розглянемо діаграму, наведену на рис. 5б. Верхній її квадрат декартов. Він визначає характеристичну стрілку $\chi_{\top}^{/}$ стрілки $\top$ на основі того, що $T^{/}$ є класифікатором підоб'єктів. Нижній квадрат також декартов.

Він визначає характеристичну стрілку для $T^{/}$, використовуючи $\top$ як класифікатор. Згідно леми про квадрати [6] зовнішній прямокутник декартовий (рис. 6).

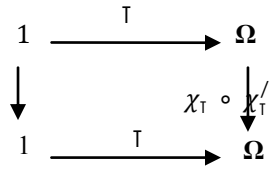


Рис. 6. Декартів квадрат класифікатору

У діаграми мається тільки одна стрілка $\Omega \to \Omega$ для якій квадрат декартовий. Оскільки для стрілки $1_\Omega: \Omega \to \Omega$ вказаний квадрат декартовий, то $\chi_\top \circ \chi_\top^{/} = 1_\Omega$. Замінюючи $\top$ на $\top^{/}$, отримуємо $\chi_\top^{/} \circ \chi_{\top/} = 1_{\Omega/}$. Таким чином, $\chi_{\top/}: \Omega^{/} \cong \Omega$. Тобто для будь-яких класифікаторів підоб'єктів один з них отримується з іншого композицією з деякою ізострілкою, яка з'єднує їх кінці.

Перехід від f до χ_f встановлює взаємно однозначні відповідності між підоб'єктами об'єкту d і стрілками $d \to \Omega$. Для цього визначимо, що для будь-яких $f: a \rightarrowtail d$ і $g: b \rightarrowtail d \Longrightarrow f \simeq g$ тільки тоді, коли $\chi_f = \chi_g$.

Допустимо, що $\chi_f = \chi_g$ (рис. 7а). Тоді зовнішній квадрат комутативний. У силу властивості універсальності внутрішнього декартового квадрату існує стрілка *k*, яка пропускає g через f. Тому $g \subseteq f$. Замінюючи місцями f і g отримуємо включення $f \subseteq g$. Тобто $f \simeq g$.

І у зворотному напрямку, пускай $f \simeq g$ і внутрішній квадрат декартовий. Тоді існує ізострілка $k: b \to a$, для якої верхній трикутник комутативний.

Використовуючи цю обставину, можна показати, що зовнішній квадрат також декартовий. Тому, як було надано вище, для монострілки *g*, отримуємо $\chi_f = \chi_g$.

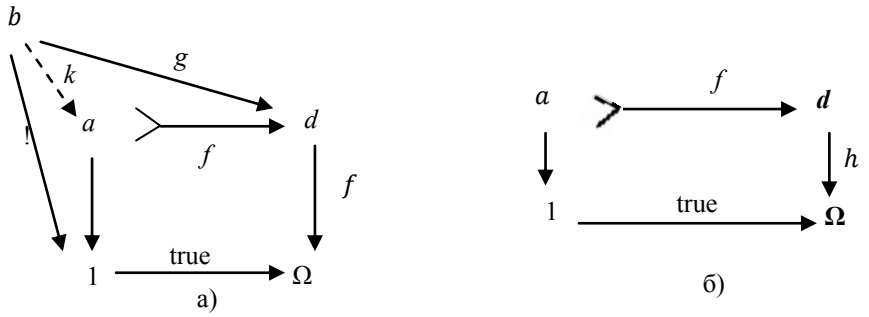


Рис. 7. а) Комутативна діаграма декартового квадрату для $f: a \rightarrowtail d$ і $g: b \rightarrowtail d \Longrightarrow f \simeq g$, коли $\chi_f = \chi_g$. б) Декартів квадрат множини β-стрілки $h: d \to \Omega$

Функція, яка співвідносить χ_f монострільці f (підоб'єкту $[f]$), вкладає Sub(d) у β(d,Ω). Крім того, якщо для вільної стрілки (рис. 7б) $h: d \to \Omega$ підняти true вдовж h, то виникає, при цьому, стрілка f, яка буде мономорфною.

Так як true – монострілка, то зворотній образ монострілки завжди сам є монострілкою. Тому h повинна співпадати з χ_f. Таким чином, у категорії, яка має класифікатори підоб'єктів $Sub(d) \cong \beta(d, \Omega)$.

На рис. 8 представлені різні варіанти побудови: Рис. 8а – для вільного β-об'єкту a композиція $\text{true} \circ 1_a$ стрілок $!: a \to 1$ і true буде визначатися через true_a або через $\top_a$, або іноді просто через true !. Рис. 8б – надано декартовий квадрат з характеристичною стрілкою для $\text{true}: 1 \rightarrowtail \Omega \Longrightarrow 1_\Omega$, тобто $\chi_{\text{true}} = 1_\Omega$. Рис. 8в – надано декартовий квадрат для $\chi_{1_\Omega} = \text{true}_\Omega = \text{true} \circ 1_\Omega$. Рис. 8г – надано діаграма для вільного $f: a \to b$.

Для визначення елементарного топосу необхідно визначити властивості множин, підмножин та категорій, при яких вони можуть бути топосами: β повинна бути кінцево повною; β повинна бути кінцево коповною; β повинна допускати експоненсування; β повинна мати класифікатор підоб'єктів. Тобто вона повинна мати кінцевий об'єкт і зворотній образ, двойковий образ якого може бути замінений умовою у якій β має початковий об'єкт і альмагами. Топос може бути визначений як декартово замкнута категорія з класифікатором об'єктів.

Розглянемо приклади топосів у категоріях: **Set** – топос. **Finset** – топос, межа, експоненсування і класифікатор підоб'єктів $\top: 1 \to \Omega$ такі як у **Set**.

Finord – топос. Кожна кінцева множина ізоморфна деякому кінцевому ординалу ($A \cong n$, якщо A має n елементів). Тому усі кате горні побудови у **Finset** переносяться у **Finord**. Класифікатор підоб'єктів у **Finord** уявляє собою ту саму функцію $\text{true}: \{0\} \to \{0,1\}$, що і у **Finset, Set.**

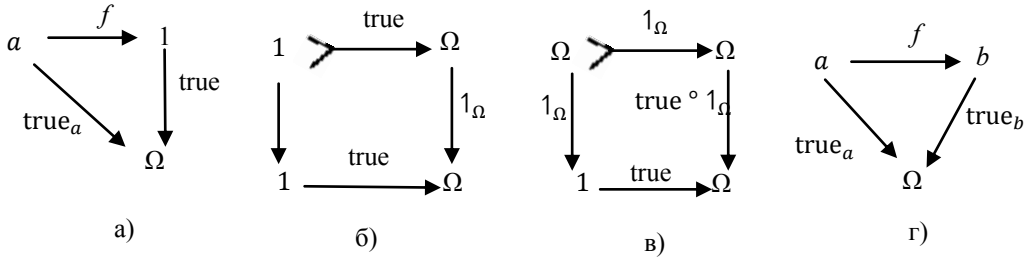


Рис. 8. Діаграми: а) для вільного β-об'єкту a композиція $true \circ 1_a$ стрілок $!: a \to 1$ і true – $true_a$; б) $true: 1 \rightarrowtail \Omega \Longrightarrow 1_\Omega$, тобто $\chi_{true} = 1_\Omega$; в) $\chi_{1_\Omega} = true_\Omega = true \circ 1_\Omega$; г) для вільного $f: a \to b$

Set^2, тобто категорія пар множин – топос. Усі конструкції отримуються "подвоюванням" відповідних конструкцій у **Set**. Кінцевим об'єктом служить пара $\langle\{0\},\{0\}\rangle$ одноелементних множин. Для даних двох стрілок $\langle f,g\rangle: \langle A,B\rangle \to \langle E,F\rangle, \langle h,k\rangle: \langle C,D\rangle \to \langle E,F\rangle$ у **Set**^{2} з загальним кінцем побудуемо у категорії **Set** декартові квадрати (рис. 9), які перетворюються у декартов квадрат, який є декартовим у **Set**^{2}.

Експоненціалом $\langle C,D\rangle^{(A,B)}$ служить пара $\langle C^A, D^B\rangle$, а стрілкою значення з об'єкту $\langle C,D\rangle^{(A,B)} \times \langle A,B\rangle = \langle C^A \times A,\ D^B \times B\rangle$ у об'єкт $\langle C,D\rangle$ – пара $\langle e,f\rangle$ відповідних стрілок значення $e: C^A \times A \to C$ і $D^B \times B \to D$ у **Set.**

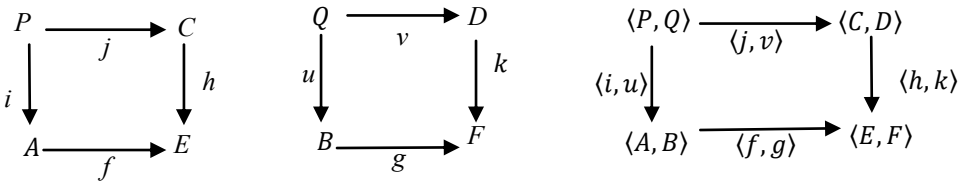
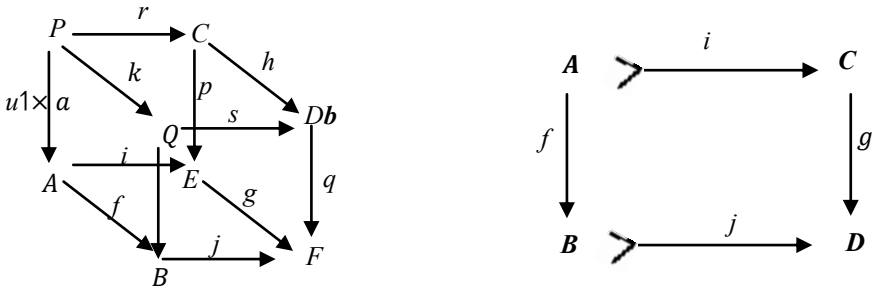


Рис. 9. Декартові квадрати: $\langle f,g\rangle\colon \langle A,B\rangle \to \langle E,F\rangle, \langle h,k\rangle\colon \langle C,D\rangle \to \langle E,F\rangle$

Пара $\langle \top,\top\rangle\colon \langle\{0\},\{0\}\rangle \to \langle 2,2\rangle$ є класифікатором підоб'єктів. Якщо β_1 і β_2 – топоси, то і добуток категорій $\beta_1 \times \beta_2$ також буде топосом. $\mathbf{Set}^{\to}$, тобто категорія функцій – топос. Кінцевим об'єктом служить тождественна функція $\mathrm{id}_{\{0\}}$ з $\{0\}$ у $\{0\}$. Що стосується зворотного образу. Розглянемо "куб", який наведений на рис. 10а.



а) б)

Рис. 10. а) Куб підоб'єктів множин. б) Комутативна діаграма монострілок у $\mathbf{Set}^{\to}$

де f, g, h – данні $\mathbf{Set}^{\to}$ об'єкти, $\langle i,j\rangle$ є $\mathbf{Set}^{\to}$ стрілка з f у g і $\langle p,q\rangle$ є $\mathbf{Set}^{\to}$ стрілка з h у g. Частина діаграми, яка осталася, отримується утворенням у **Se**t декартових квадратів, а стрілка k виникає в силу властивості універсальності зворотного образу стрілок j і q. Тоді $\mathbf{Set}^{\to}$ стрілки $\langle u,v\rangle$ і $\langle r,s\rangle$ складають зворотний образ стрілок $\langle i,j\rangle$ і $\langle p,q\rangle$.

Що стосується класифікатора. Якщо $f\colon A \to B$ – підоб'єкт $g\colon C \to D$ у $\mathbf{Set}^{\to}$ і пара $\langle i,j\rangle$ є $\mathbf{Set}^{\to}$-монострілкою з f у g, то її компоненти будуть монострілками у **Set** і має місце комутативна діаграма, яка наведена на рис. 10б.

Можна вибрати монострілки i і j дійсними включеннями так, що $A \subseteq C, B \subseteq D$ і f є обмеженням g, тобто $f(x) = g(x)$ для усіх $x \in A$. Отримується наступна картина, представлена на рис. 11.

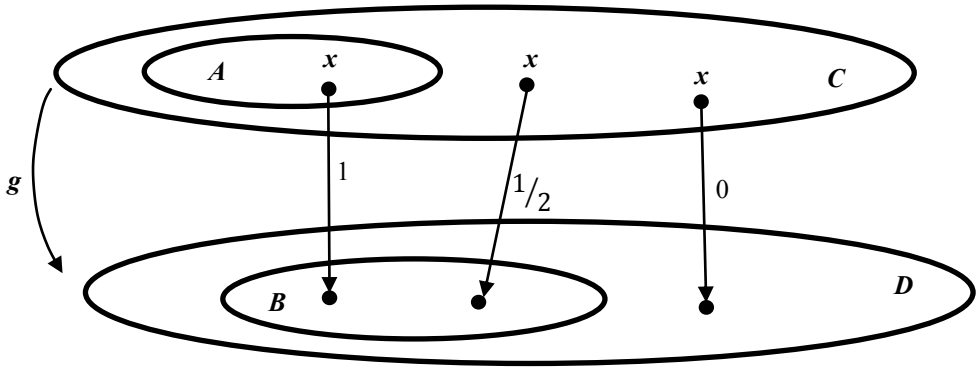


Рис. 11. Множини у $\mathbf{Set}^{\to}$ при $A \subseteq C, B \subseteq D$

Елементи x з множини C можна розкласти на три наступних класу:

$x \in A$; 2. $x \notin A$, але $g(x) \in B$; 3. $x \notin A$ і $g(x) \notin B$. Таким чином вводиться триелементна множина $\{0,\ 1/2,\ 1\}$ і визначимо $\Psi\colon C \to \{0,\ 1/2,\ 1\}$ наступними умовами:

$$\Psi(x) = \begin{cases} 1, \text{якщо має місце 1 клас,} \\ 1/2\text{, якщо має місце 2 клас,} \\ 0, \text{якщо має місце 3 клас.} \end{cases} \quad (2)$$

Побудуємо куб, який наведений на рис. 12., де $\mathrm{true}(0) = t'(0) = 1$ і $t(0) = 0,\ t(1) = t(1/2) = 1$. Через x_B позначена характеристична функція множини B.

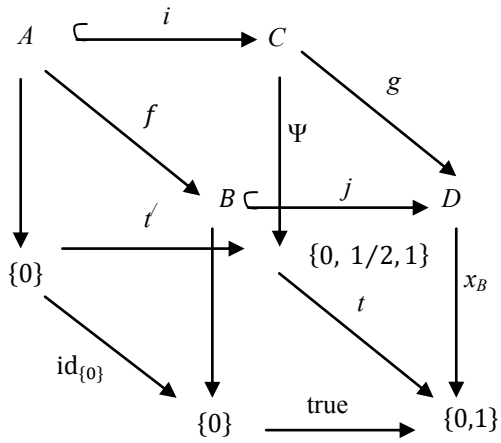


Рис. 12. Куб підоб'єктів множин для $\Psi: C \to \{0,\ 1/2,\ 1\}$

Нижня грань кубу уявляє собою класифікатор підоб'єктів $\top: 1 \to \Omega$ у $\mathbf{Set}^{\to}$. Пара $\langle t', \mathrm{true}\rangle$ є $\mathbf{Set}^{\to}$-стрілкою з $1 = id_{\{0\}}$ у $\Omega = t: \{0,\ 1/2,\ 1\} \to \{0,1\}$. Передня і задні грані кубу є декартовими квадратами у **Set**. Уся діаграма показує, що пара $\langle \Psi, x_B\rangle$ є характеристичною $\mathbf{Set}^{\to}$-стрілкою монострілки $\langle i, j\rangle$.

Заключення

У подальшому виникає питання визначення пучків топосів та їх розділення. Усі ці питання необхідно розглядати у комплексі розкриваючи просторові топоси у підмножинах та підоб'єктах просторового взаємовідношення стрілок, функцій з метою подальшого розкриття питань взаємодії загрозливих впливів на об'єкти та підоб'єкти множин механізмів захисту інформації.

Література

1. Павлов І.М. В.О. Композиція і категорії функцій систем загроз в областях систем захисту інформації / І.М. Павлов. В.О. Бірюков, – Захист інформації. – № 1. – 2013. – С. 28 – 37.

2. Павлов І.М. Морфізм функцій і бієктивність об'єктів при проекції множин загроз та областей систем захисту інформації / І.М. Павлов. – Сучасна спеціальна техніка. – № 1. – 2013. – С. 36 – 45.

3. Павлов І.М. Проектування комплексних систем захисту інформації / І.М. Павлов, В.О. Хорошко. – К.: 2011. – 245 с.

4. Manes E. G. Category Theory Applied to Computation and Control, Lecture Notes in Computer Science, Vol. 25, Springer-Verlag, 1996.

5. Аксиоматична теорія множин: навч. посіб. / М.М. Попов. – Чернігівський національний університет (ЧНУ). – 2011. – 79 с.

6. Grayson. R. Heyting-valued models for intuitionistic set theory. – Lecture Notes in Mathematics. 2002, p. 402.

References

1. Pavlov I.M. V.O. Kompozicija i kategorii funkcij sistem zagroz v oblastjah sistem zahistu informacii / I.M. Pavlov. V.O. Birjukov, – Zahist informacii. – № 1. – 2013. – S. 28 – 37.

2. Pavlov I.M. Morfizm funkcij i biєktivnist' ob'єktiv pri proekcii mnozhin zagroz ta oblastej sistem zahistu informacii / I.M. Pavlov. – Suchasna special'na tehnika. – № 1. – 2013. – S. 36 – 45.

3. Pavlov I.M. Proektuvannja kompleksnih sistem zahistu informacii / I.M. Pavlov, V.O. Horoshko. – K.: 2011. – 245 s.

4. Manes E. G. Category Theory Applied to Computation and Control, Lecture Notes in Computer Science, Vol. 25, Springer-Verlag, 1996.

5. Aksiomatichna teorija mnozhin: navch. posib. / M.M. Popov. – Chernigivs'kij nacional'nij universitet (ChNU). – 2011. – 79 s.

6. Grayson. R. Heyting-valued models for intuitionistic set theory. – Lecture Notes in Mathematics. 2002, p. 402.

Павлов И.Н.

ПОНЯТИЕ КЛАСИФИКАТОРОВ И ТОПОС В ПОДОБЪЕКТОВ МНОЖЕСТВ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

В статье рассматривается категорный анализ взаимоотношений множеств и подмножеств с целью проведения пространственного анализа угрожающих воздействий на системы защиты информации.

Ключевые слова: *множества, подмножества, объекты, подобъекты, система защиты информации,топос, функции.*

Pavlov I.

CONCEPT CLASSIFIER AND TOPOS IN UNDER OBJECTS SETS OF INFORMATION SECURITY

The article deals with the analysis of categorical relationship sets and subsets to conduct spatial analysis threatening impacts on information security system.

Keywords: *multitude, subset, objects, under objects, system protection information, topos, functions.*

Павлов Ігор Миколайович, кандидат технічних наук, доцент, начальник кафедри тактико-спеціальної підготовки Військового інституту телекомунікацій та інформатизації Національного технічного університету України "Київський політехнічний інститут".

Рецензент: Осенин Юрий Иванович - д.т.н., профессор, ВНУ им. В. Даля.