УДК 004.415.056.5(075)

І.М. Павлов[1], В.О. Хорошко[2]

[1]к.т.н, доцент ВІТІ НТУУ "КПІ"
[2]д.т.н, професор НАУ

ФУНКТОРНІСТЬ ТА ГРАНІЧНІСТЬ ВІДОБРАЖЕНЬ ОБ'ЄКТІВ МНОЖИН В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

У статті розглядаються математичні основи категорій логіки взаємин загроз і областей системи захисту інформації при ескізному проектуванні систем захисту інформації.
Ключові слова: функторность, категорії, множини, підмножини, об'єкти, функції, система захисту інформації, граничность.

Вступ

Результативне рішення задач аналізу і синтезу СЗІ не може бути забезпечено одними лише способами простого опису їх поведінки в різних умовах – системотехніка видвігає проблеми, які потребують кількісні оцінки характеристик. Такі дані, які отримані експериментально або шляхом математичного *моделювання*, повинні розкривати властивості СЗІ. Основним з них є ефективність, під якою розуміється ступінь відповідності результатів захисту інформації поставленій меті. Остання, в залежності від ресурсів, які маються, знань розробників та інших факторів, може бути досягнута в тій або іншій мірі, при цьому можливі альтернативні шляхи її реалізації. Ефективність має безпосередній зв'язок з іншими системними властивостями, в тому числі надійністю, живучістю, завадозахіщеністю – а в цілому стійкістю. Тому кількісна оцінка ефективності дозволяє вимірювати і об'єктивно аналізувати основні властивості систем на всіх стадіях їх життєвого циклу, починаючи з етапу формування вимог і ескізного *проектування*.

У [1, 2] авторами запропоновані основи категорійного апарату теорії множин, які дозволяють пояснити процес взаємовідносин множин загроз и множин системи захисту інформації, який дозволяє будувати різни математичні моделі з метою аналізу систем інформаційного обміну в системах критичного застосування.

Постановка проблеми

Під час визначення взаємовідносин множин та підмножин загроз та системи захисту інформації виникає проблема побудови внутрішніх взаємозв'язків, при яких змінюється якісні і кількісні показники ефективности захисту інформації. Побудова математичних моделей взаємовідносин множин передбачає чіткі підходи до визначення основ аналізу взаємовідносин цих множин [3]. Це в першу чергу стосується функторності та граничності самих множин та підмножин, що і є *метою цієї статті*.

Основна частина

Нехай d – деяка підмножина множини C, яка має функції g, h. Тоді теоретико-множинні функції $h,g: C \to A \Longrightarrow f: A \to B$ є ін'єктивні або взаємно однозначні, коли не існує двох різних входів, які мають один і той-же вихід [5], тобто коли для будь-яких $x, y \in A$ з $f(x) = f(y) \Longrightarrow x = y$.

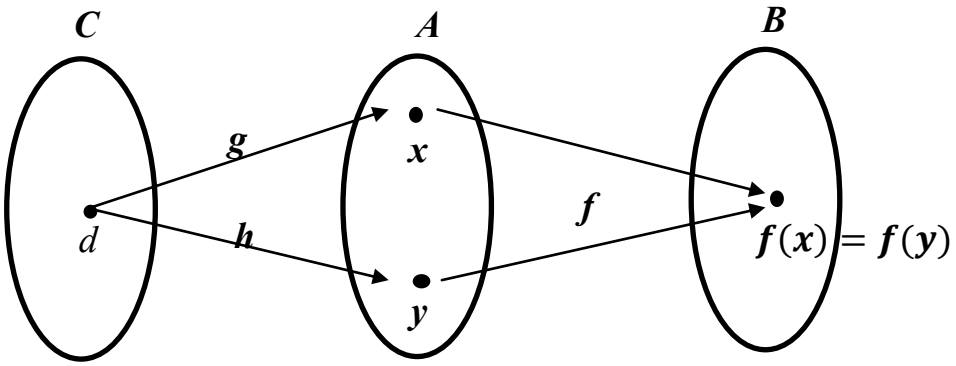


Рис. 1. Модель побудови ін'єктивної функції
або мономорфної стрілки

Якщо визначити, що $f: A \to B$ ін'єктивна (рис. 2):

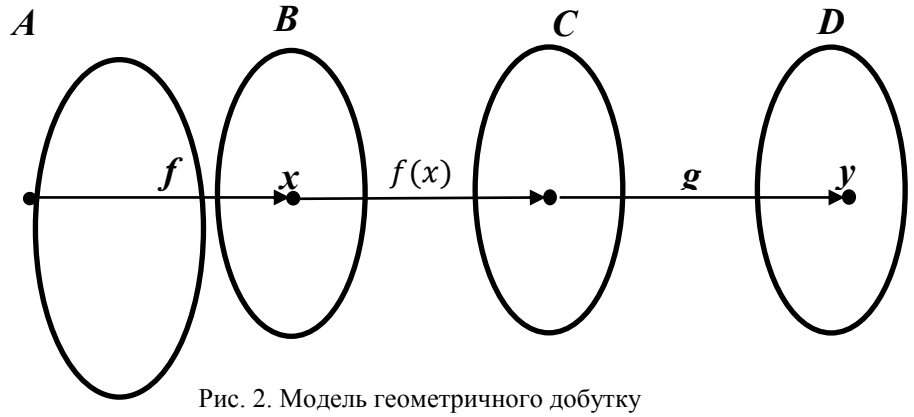


Рис. 2. Модель геометричного добутку
теоретико-множинних функцій

Для даних теоретико-множинних функцій $f: A \to B$ та $g: C \to D$ визначається функція $f \times g$ з $A \times C$ до $B \times D$ рівнянням:

$$f \times g(\langle x, y\rangle) = \langle f(x), g(y)\rangle. \quad (1)$$

З (1) бачимо, що $f \times g$ є добутком двох композицій $f \circ pr_A: A \times C \to A \to B$ та $g \circ pr_C: A \times C \to C \to D$. *Функторним* називають добуток відображень (проекцій) [4]. Тому:

Якщо $f: a \to b$ та $g: c \to d$ – дві β стрілки, то через $f \times g: a \times c \to b \times d$ визначимо β-стрілку $\langle f \circ pr_a,\ g \circ pr_c\rangle$. На рис. 3 надана композиція функторних відображень при: $\langle f \circ pr_a,\ g \circ pr_c\rangle$.

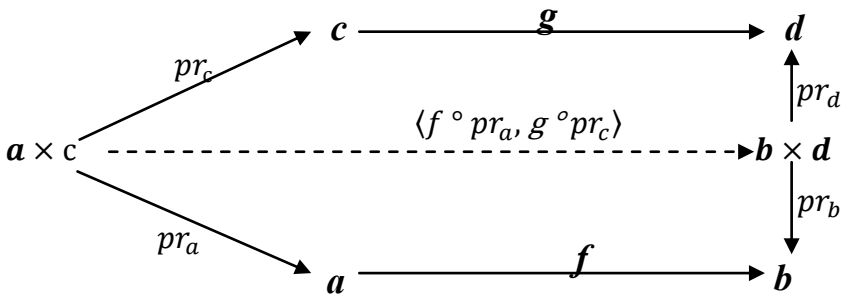


Рис. 3. Комутативна діаграма композиції функторних тождественних підмножин

При $1_a \times 1_b = 1_{a \times b}$ тождественна діаграма функторних відображень має вигляд наданий на рис. 4.

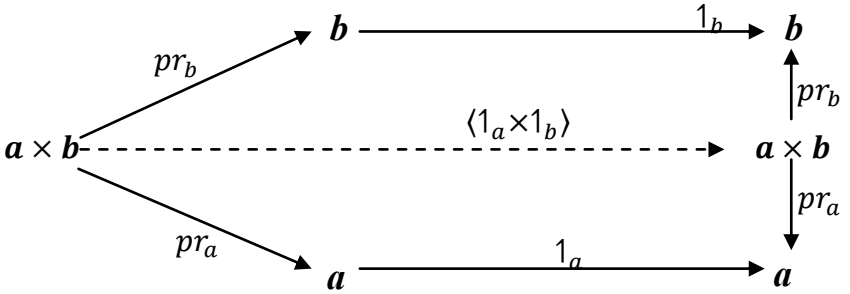


Рис. 4. Комутативна діаграма функторних відображень при $1_a \times 1_b = 1_{a \times b}$

При $(a \times b) \times c \cong a \times (b \times c)$ тождественна діаграма функторних відображень бути мати вигляд наданий на рис. 5.

У наданих діаграмах пунктирна стрілка означає, що існує одна і тільки одна стрілка, яка займає вказане положення, при якому діаграма стає комутативною.

Для визначення граничності множин розглянемо поняття добутку множин на випадок 3-х співмножників, визначивши $A \times B \times C$ як множину упорядкованих трійок $\langle x, y, z \rangle$ у яких: $A \times B \times C = \{\langle x, y, z \rangle : x \in A, y \in B, z \in C\}$.

Покладемо множини *A*, *B*, *C* рівними послідовності $A = \langle x_1, x_2, \dots, x_m \rangle$, $B = \langle y_1, y_2, \dots, y_v \rangle$, $C = \langle z_1, z_2, \dots, z_r \rangle$. У цьому випадку отримуємо *m*, *v*, *r* – кратний добуток множин *A*, *B*, *C* на себе:

$$A^m = \{\langle \overline{x_1, x_m} \rangle : x_1, x_2, \dots, x_m \in A\},$$
$$B^v = \{\langle \overline{y_1, y_v} \rangle : y_1, y_2, \dots, y_v \in B\},$$
$$C^r = \{\langle \overline{z_1, z_r} \rangle : z_1, z_2, \dots, z_r \in C\}. \quad (2)$$

Поставимо у відповідність множинам A^m, B^v, C^r різні відображення проекцій і отримуємо матричні вирази:

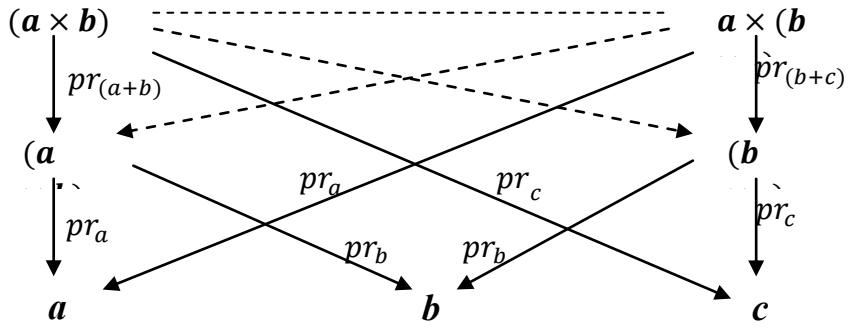


Рис. 5. Комутативна діаграма ізоморфності функторних відображень тождественних підмножин при $(a \times b) \times c \cong a \times (b \times c)$

$$A^m = \begin{matrix} pr_1^m(\langle x_1 \rangle) = x_1 \\ pr_2^m(\langle x_1, x_2 \rangle) = x_2 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ pr_m^m(\langle x_1, x_2, \dots, x_m \rangle) = x_m \end{matrix}$$

$$B^v = \begin{matrix} pr_1^v(\langle y_1 \rangle) = y_1 \\ pr_2^v(\langle y_1, y_2 \rangle) = y_2 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ pr_y^v(\langle y_1, y, \dots, y_v \rangle) = y_v \end{matrix} \qquad (3)$$

$$C^r = \begin{matrix} pr_1^r(\langle z_1 \rangle) = z_1 \\ pr_2^r(\langle z_1, z_2 \rangle) = z_2 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ pr_r^r(\langle z_1, z_2, \dots, z_m \rangle) = z_r \end{matrix}$$

Якщо уявити множини у складі підмножин та стрілок між ними, то можна представити, що для будь-яких довільних β-стрілок $f_{\overline{1,m}}: a \to c$, які мають загальний початок, існує одна і тільки одна стрілка $\langle f_1, \dots, f_m \rangle$, для якої діаграма, яка надана на рис. 6. комутативна.

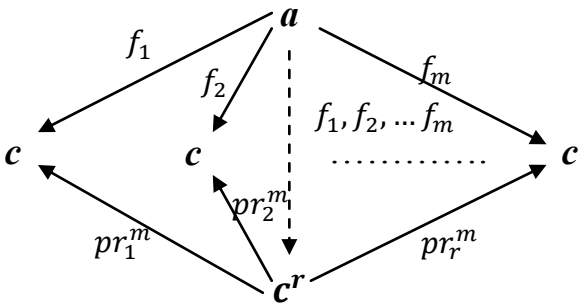


Рис. 6. Комутативна діаграма кінцевості функторних відображень тождественних підмножин

Для $m = 1$ у якості a^1 береться первинна підмножина та $pr_1^1: a_1 \to a_1 = 1_a$.

Кінцеві добутки будуть грати важливу роль у семантиці першого порядку елементарної істинності.

Двійчастим до поняття добутку є поняття *кодобутку*, або суми об'єктів. Його визначення отримується безпосередньо з визначення добутку за принципом двійчастості [5].

Кодобутком у категорії β двох об'єктів a і b називають β-об'єкт, який позначають через $a + b$, сумісно з парою $(i_a: a \to a + b, i_b: b \to a + b)$ β-стрілок, такий, що для вільної пари $(f: a \to c, g: b \to c)$ β-стрілок існує одна і тільки одна стрілка $[f,g]: a + b \to c$, для якої комутативна діаграма, яка надана на рис. 7.

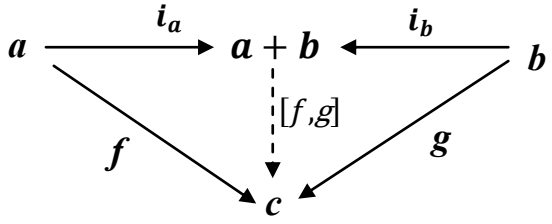


Рис. 7. Комутативна діаграма кодобутку ізоморфних підмножин $dob: c \to a \times b$

Тобто $[f,g] \circ i_a = f$ і $[f,g] \circ i_b = g$. Стрілка $[f,g]$ має назву кодобутку стрілок f і g відносно ін'єкцій i_a і i_b.

У категорії усіх множин **Set** кодобуток об'єктів A і B – це їх диз'юнктне об'єднання $A+B$, тобто об'єднання двох множин, ізоморфних A і B відповідно, але які не перетинаються. Точніше, якщо:

$$A' = \{\langle a, 0\rangle: a \in A\} = A \times \{0\},$$
$$B' = \{\langle b, 1\rangle: b \in B\} = B \times \{1\}, \quad (4)$$

то отримуємо $A + B = A' \cup B'$.

Ін'єкції $i_A: A \to A + B$ та $i_B: B \to A + B$ визначаються правилами: $i_A(a) = \langle a, 0\rangle, i_B(b) = \langle b, 1\rangle$ відповідно.

У категорії передпорядку $(P, \sqsubseteq)$ [2] кодобуток $p + g$ визначається наступними властивостями:

– $p \sqsubseteq p + g$, $g \sqsubseteq p + g$ тобто $p + g$ є верхньою гранню для p і g;

– якщо $p \sqsubseteq c$ і $g \sqsubseteq c$, то $p + g \sqsubseteq c$, тобто $p + g$ менше, за будь-яку іншу грань для p і g.

Таким чином, $p + g$ є найменшою верхньою гранню для p і g – $p \sqcup g$. У частково-упорядкованій множині найменша верхня грань одна у випадку коли вона існує.

У *решітки* – скелетальній категорії передпорядку, у якій існує добуток і кодобуток будь-яких двох її об'єктів утворюється найменша верхня грань і найменша нижня грань.

Відповідно виникає питання визначення *прирівнювача* (рос. уравнителя).

Якщо $f,g: A \rightrightarrows B$ – пара паралельних функцій [1] у категорії усіх множин **Set** і a – підмножина у A, яка складається з усіх елементів, на яких f і g співпадають, тобто $E = (x: x \in A \text{ і } f(x) = g(x))$. Тоді функція $i: E \hookrightarrow A$ включення є *прирівнювач* функцій f і g. Основою для цього є те, що під час композиції цих функцій з i отримується рівняння

$f \circ i = g \circ i$, тобто i "прирівнює" ці функції. Більш того, і є "каноничним" прирівнітелем для f і g. Це означає, що якщо $h: C \to A$ – вільний інший такий прирівнювач, тобто $f \circ h = g \circ h$, то h однозначно "пропускається" через $i: E \hookrightarrow A$, тобто існує одна єдина функція $k: C \to E$, така, що $i \circ k = h$ (рис. 8).

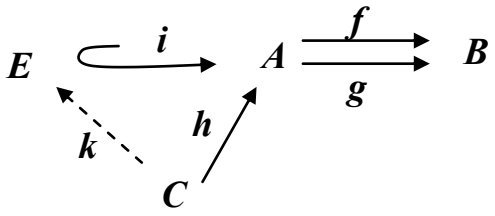


Рис. 8. Комутативна діаграма прирівнювача ізоморфних підмножин $dob: c \to a \times b$

Для будь-якої цієї стрілки h існує одна **Set**-стрілка, підстановка якої замість пунктирної стрілки робить діаграму комутативною. Тобто, якщо $i \circ k$ співпадає з h, то для будь-якого $c \in C$ має місце рівняння $i\big(k(c)\big) = h(c)$, тобто $k(c) = h(c)$ (так як i - включення).

У якості висновку маємо:

Стрілка $i: e \to a$ з категорії β може бути прирівнювачем пари $f, g: a \to b$ β-стрілок, якщо: $f \circ i = g \circ i$;

Для будь-якої β-стрілки $h: c \to a$ яка задовольняє рівнянню $f \circ h = g \circ h$, існує тільки одна β-стрілка $k: c \to e$, така, що $i \circ k = h$.

Для визначення поняття *коприрівнювача* необхідно розібратися з поняттями межи та комежи (рос. предела и копредела).

Введемо діаграму D у категорії β, під якою розуміється сукупність об'єктів $d_i, d_j, \ldots$ сумісно з деякими β-стрілками $g: d_i \to d_j$ між ними (рис. 9а).

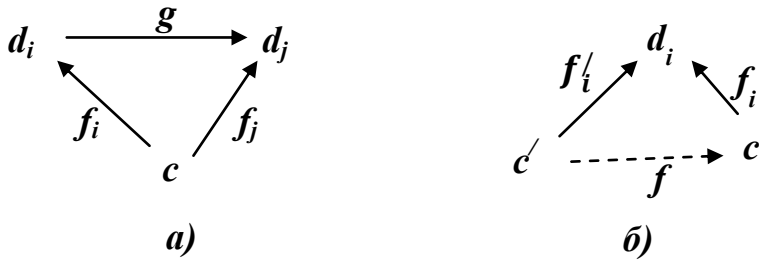


Рис. 9. Комутативна діаграма а) конусу, б) межі

Тобто для діаграми D конус: $\{f_i: c \to d_i\}$.

Межа діаграми D це D-конус $\{f_i: c \to d_i\}$, такий, що для будь-якого іншого D-конусу $\{f_i': c' \to d_i\}$ існує одна і тільки одна стрілка $f: c' \to c$, для якої діаграма комутативна при кожному d_i з D (рис. 9б).

Для прикладу можна привести наступний:

Нехай D – діаграма, у якій є пара паралельних векторів $g, f: a \rightrightarrows b$, тоді D-конус –

це пара $h: c \to a,\ j: c \to b$, для яких комутативні діаграми, які представлені на рис. 10.

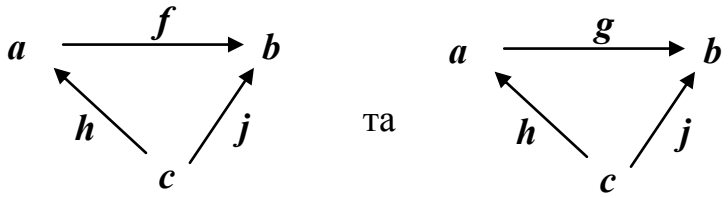
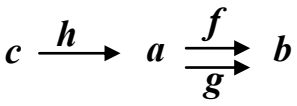


Рис. 10. Комутативні діаграми *D*-межі

Це дає $j = f \circ h = g \circ h$. Тому можна говорити, що *D*-конус, у цьому випадку – це стрілка $h: c \to a$, для якої твердження, описується комутативної діаграмою:



Тобто *D*-межа – це прирівнювач пари стрілок *f* та *g*.

Двойковим зразком визначається коконус $\{f_i: d_i \to c\}$ для діаграми *D*, яка складається з об'єкта c і стрілок $f_i: d_i \to c$, по одній для кожного об'єкта d_i з *D*, які задовольняють умовам комутативності.

Комежа для *D* – це коконус $\{f_i: d_i \to c\}$ з властивостями коуніверсальності, такими, що для будь-якого іншого коконуса $\{f_i^{/}: d_i \to c^{/}\}$ існує єдина одна стрілка $f: c \to c^{/}$ така, що для кожного d_i з *D* діаграма комутативна (рис. 9б).

Коприрівнювачем пари паралельних β-стрілок *f, g* є комежа $g, f: a \rightrightarrows b$. Коприрівнювач можна розглядати як таку β-стрілку $q: b \to c$ при якій: $q \circ f = q \circ g$ та будь-якої стрілки $h: b \to c$, задовольняє рівнянню $h \circ f = h \circ g$, існує одна єдина стрілка $k: e \to c$, для якої діаграма комутативна (рис. 11).

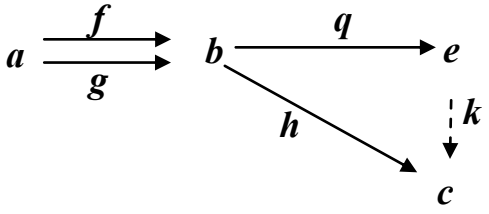


Рис. 11. Комутативна діаграма коприрівнювача
ізоморфних підмножин $dob: c \to a \times b$

У категорії **Set** коприрівнювач описують у термінах відносин $\in$ за допомогою важливого поняття відношення еквівалентності [6].

Відношення еквівалентності на множині $\boldsymbol{A}$ по визначенню – відношення $R \subseteq \boldsymbol{A} \times A$ має наступні властивості:

– рефлективності, тобто aRa для кожного $a \in A$;
– транзитивності, тобто якщо aRb і bRc то aRc для будь-яких a, b, c з *A*;

– симетричністю, тобто якщо aRb, то bRa для будь-яких a і b з A.

Процес ототожнення еквівалентних множин впроваджується в об'єднання цих множин у одну множину при поєднанні їх друг з другом відношенням еквівалентності. Сукупності, які виникають розглядаються, при цьому, як нові відношення. Формально для $a \in A$ визначається клас R-еквівалентності як множина:

$$[a] = \{b: aRb\}, \tag{4}$$

усіх елементів з A, які знаходяться у R-відношенні до a. Одна і таж множина може бути класом еквівалентності різних елементів. У загальному випадку:

– $[a] = [b]$ тоді і тільки тоді, коли aRb. Тобто два еквівалентних елемента знаходяться у відношенні R з однією і той-же множиною елементів.

– Якщо $[a] \neq [b]$, то $[a] \cap [b] = \emptyset$. Тобто два різних класу еквівалентності не мають загальних елементів.

– $a \in [a]$. Тобто кожна $a \in A$ є елементом одного і того-ж класу R-еквівалентності.

Процес ототожнення складається у переході від цієї множини до нової, елементами якої є класи R-еквівалентності, тобто розглядається перехід від множини A до множини:

$$A/_R = \{[a]: a \in A\}. \tag{5}$$

Цей перехід виконується за допомогою природного відображення $f_R: A \to A/_R$, де $f_R(a) = [a]$, для $a \in A$.

Якщо aRb, то $f_R(a) = f_R(b)$, тобто функція f_R ототожнює R-еквівалентні елементи.

Функція f_R є коприрівнювачем пари $f, g: R \rightrightarrows A$ функцій проектування з R до A, тобто які задаються рівняннями,

$$f(\langle a, b\rangle) = a \text{ і } g(\langle a, b\rangle) = b. \tag{6}$$

Представимо діаграму природного відображення коприрівнювача, наведену на рис. 12 при заданій стрільці k, яка задовольняє рівнянню: $h \circ f = h \circ g$ при цьому $k \circ f_R = h$. Тоді для будь – якого $[a] \in A/_R$ будемо мати $k([a]) = k(f_R(a)) = k \circ f_R(a) = h(a)$.

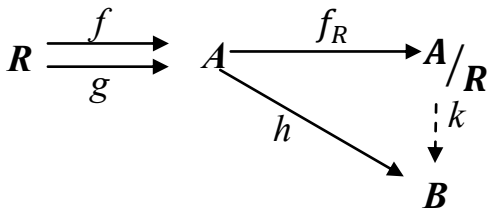


Рис. 12. Комутативна діаграма коприрівнювача природного відображення множин

Відношення еквівалентності можна використовувати для побудови у **Set** копрірівнювачів. Щоб побудувати копрірівнювач пари функцій $f,g: R \rightrightarrows A$ необхідно ототожнити $f(x)$ з $g(x)$ для $x \in A$ згідно відношення:

$$S = \{\langle f(x), g(x)\rangle : x \in A\} \subseteq B \times B. \quad (7)$$

Відношення S може не бути відношенням еквівалентності на B. Однак можна розширити S до відношення еквівалентності і причому мінімальним чином. Існує відношення еквівалентності R на B, таке, що $S \subseteq R$ і якщо T – будь-яке відношення еквівалентності на B, при якому S мається у T, то $R \subseteq T$. Тобто R – найменше відображення еквівалентності на B, яке має S. Природне відображення $f_R: B \to {}^{B}/_{R}$ буде копрірівнювачем f і g.

Заключення

Розглянуті стандартні теоретико-множинні конструкції дозволяють представити взаємовідносини різних множин та підмножин, які маються як в областях загроз, так і в областях захисту систем захисту інформації. Під час ескізного проектування систем захисту інформації проектувальнику необхідно мати уяву про процеси взаємовідносин цих областей множин. Будь-яка множина, яка взаємодіє (впливає на) з іншою множиною (підмножиною) за відомими законами перетворює різні процеси, з метою реалізації тих або інших цілей, з якими створювалася та або інша множина (підмножина). Знання цих процесів дозволяють впливати на інформаційні потоки і перетворювати процеси з метою захисту інформації, яка може бути перекручена або зовсім знищена [7].

В подальшому будуть розглянуті поняття зворотнього образу, прообразу, ядерних відношень амальгам і повноти, які охоплюють усі побудови в тих або інших категоріях множин та підмножин. Це важливо для з'ясування понять експоненсування множин.

Література

1. Павлов І.М. 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. – Сучасний захист інформації. – № 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.
7. Павлов І.М. Формальное описание процесса проектирования комплексных систем защиты информации в информационно-телекоммуникационных системах / І.М. Павлов, Г.Д. Радзівілов. – Вісник ДУІКТ. − Київ.: 2010. − Т.8. − №1. − С.84 – 93.

Надійшла до редколегії 11.05.2013 р.

Рецензент: д.т.н., проф. Петров А.С.

Павлов И.Н., Хорошко В.А.

ФУНКТОРНОСТЬ И ГРАНИЧНОСТЬ ОТОБРАЖЕНИЙ ОБЬЕКТОВ МНОЖЕСТВ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

В статье рассматриваются математические основы категорий логики взаимоотношений угроз и областей системы защиты информации при эскизном проектировании систем защиты информации.

Ключевые слова: функторность, категории, множества, подмножества, обьекты, функции, система защиты информации, граничность.

Pavlov I., Horoshko V.

FUNCTORIAL AND BOUNDARY OF REFLECTIONS OF OBJECTS FROM SETS IN INFORMATION SECURITY SYSTEMS

The article deals with the mathematical foundations of the categories of logic relationships threats and areas of information security system for the schematic design of secure information systems.

Keywords: functorial, categories, sets, subsets, objects, functions, security system, the boundary.