УДК 004.415.056.5(075)

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 1, pp. 50-60

АМАЛЬГАМИ, ПОВНОТА ДІАГРАМ ТА ПІДОБ'ЄКТИ МНОЖИН В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

І.М. Павлов

Національний технічний університет України «Київський політехнічний інститут»,
просп. Перемоги, 37, Київ, 03056, Україна; e-mail: pavlov@ukr.net

У статті розглядаються математичні моделі взаємовідносин множин та підмножин на основі аналізу категорій логіки з метою подальшого проведення аналізу загроз на системи захисту інформації. Наведено опис зворотного образу, ядерних відношень та амальгам у множинах систем захисту інформації.

Ключові слова: амальгами, множина, підмножина, об'єкти, підоб'єкти, функції, система захисту інформації

Вступ

Наявні математичні моделі процесів нападу на інформацію та її захисту, на яких ґрунтуються оцінки рівня захищеності інформації у системах захисту інформації, не враховують динаміку зміни множин можливих несанкціонованих втручань і варіацій їх параметрів як у реальному масштабі часу, так і у процесі експлуатації інформаційних систем.

Моделювання у загальному розумінні та моделювання процесів нападу на інформацію у конкретному випадку є одним із ефективних методів дослідження поведінки технічних об'єктів при реалізації антагоністичних прагнень суб'єктів інформаційного конфлікту.

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

Мета дослідження

Під час моделювання процесів нападу на інформацію та процесів блокування таких нападів у будь-яких конфліктних множинах виникає проблема опису конфлікту з метою розкриття тих або інших напрямків побудови різних множин у системах захисту інформації для найбільш ефективного перекриття множин загроз живучими множинами механізмів захисту [3], для чого необхідний опис зворотного образу, ядерних відношень та амальгам у множинах систем захисту інформації, що і є *метою* цієї статті.

Основна частина

У множинах та підмножинах коамальгамою або зворотнім образом пари $a \overset{f}{\rightarrow} c \overset{g}{\leftarrow} b$ β-стрілок з загальним кінцем можна уявити межу у β-діаграми, яка представлена на рис. 1.

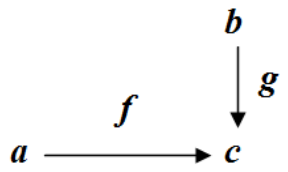

Рис. 1. β-діаграма пари стрілок $a \overset{f}{\rightarrow} c \overset{g}{\leftarrow} b$

Конус для цієї діаграми складається з 3-х стрілок f', h, g', для яких комутативна діаграма, надана на рис. 2(а).

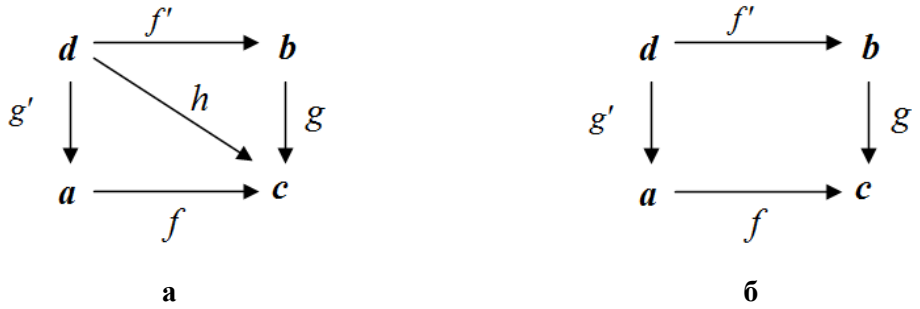

Рис. 2. Комутативні діаграми пари $a \overset{f}{\rightarrow} c \overset{g}{\leftarrow} b$: а – з 3-х стрілок f', h, g'; б – з 2-х стрілок f', g'

Це означає, що $h = g^{\circ} f' = f^{\circ} g'$. Тому можна казати, що конусом є пара $a \overset{g'}{\leftarrow} d \overset{f'}{\rightarrow} b$ β-стрілок, для яких квадрат, наданий на рис. 2(б), комутативний, тобто $f^{\circ} g' = g^{\circ} f'$.

Таким чином, згідно визначення універсальності конусу, зворотнім образом пари $a \overset{f}{\rightarrow} c \overset{g}{\leftarrow} b$ буде пара β-стрілок $a \overset{g'}{\leftarrow} d \overset{f'}{\rightarrow} b$, яка має наступні властивості [4, 5]: $f^{\circ} g' = g^{\circ} f'$, та для будь-яких $a \overset{h}{\leftarrow} e \overset{j}{\rightarrow} b$, таких, що $f^{\circ} h = g^{\circ} j$, існує і при тому тільки одна стрілка $k : e \rightarrow d$, яка задовольняє рівнянню $h = g'^{\circ} k$ і $j = f'^{\circ} k$.

Іншою мовою, для будь-яких h і j, для яких зовнішній квадрат (тобто кордон наведеної на рис. 3 діаграми) комутативний, мається одне доповнення цієї діаграми стрілкою k, при якому уся діаграма стає комутативною.

Зовнішній квадрат f, g, f', g' цієї діаграми ще має назву декартового квадрату. У цьому випадку можна казати, що f' — зворотній образ f відносно g і що f' отримується підйомом f вдовж g, а g' — зворотній образ g відносно f і отримується підйомом g вдовж f.

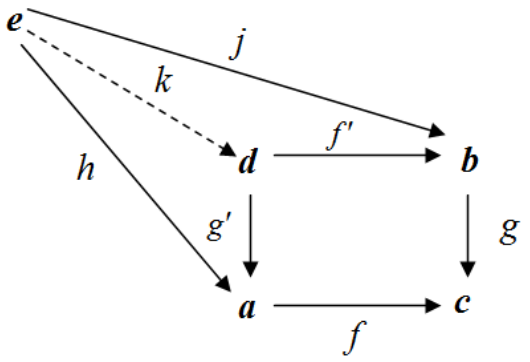

Рис. 3. Комутативні діаграми пари зворотного образу $a \overset{h}{\leftarrow} e \overset{j}{\rightarrow} b$ для рівнянь $h = g'^{\circ}k$ і $j = f'^{\circ}k$

У **Set** [6] зворотній образ двох теоретико-множинних функцій f і g визначається рівняннями (рис. 4):

$$D = \{\langle x, y\rangle : x \in A,\ y \in B \text{ і } f(x) = g(y)\}$$
$$f'(\langle x, y\rangle) = y, \quad g'(\langle x, y\rangle) = x. \tag{1}$$

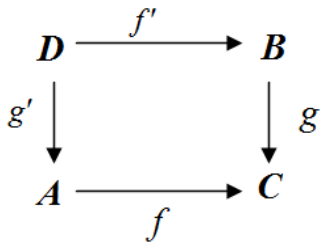

Рис. 4. Комутативна діаграма теоретико-множинних функцій

Таким чином, D є підмножиною добутку $A \times B$, а f' і g' — функції проектування. І D — є добутком A і B над C $\left(A \underset{C}{\times} B\right)$.

Якщо $f : A \rightarrow B$ — довільна функція і C — деяка підмножина у B, то можна уявити *прообразом множини* C при відображенні f (ще позначають, як $f^{-1}(C)$) підмножину у A, яка складається з усіх тих елементів $x \in A$, для яких $f(x) \in C$, тобто:

$$f^{-1}(C) = \{x : x \in A \text{ і } f(x) \in C\}. \tag{2}$$

Формула (2) представлена діаграмою, наведеною на рис. 5.

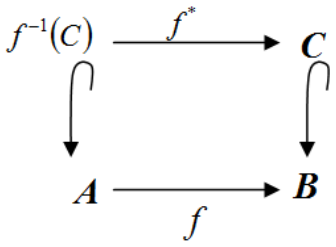

Рис. 5. Комутативна діаграма прообразу множини C при відображенні f

У діаграмі, яка наведена на рис. 5, стрілки із зігнутими кінцями визначають включення, а f^* визначається рівнянням $f^*(x) = f(x)$ для $x \in f^{-1}(C)$. Тобто f^* — обмеження функції f на $f^{-1}(C)$ є декартовим квадратом у категорії **Set**. Таким чином, прообраз C при відображенні f отримується підйомом C вздовж f (рис. 6).

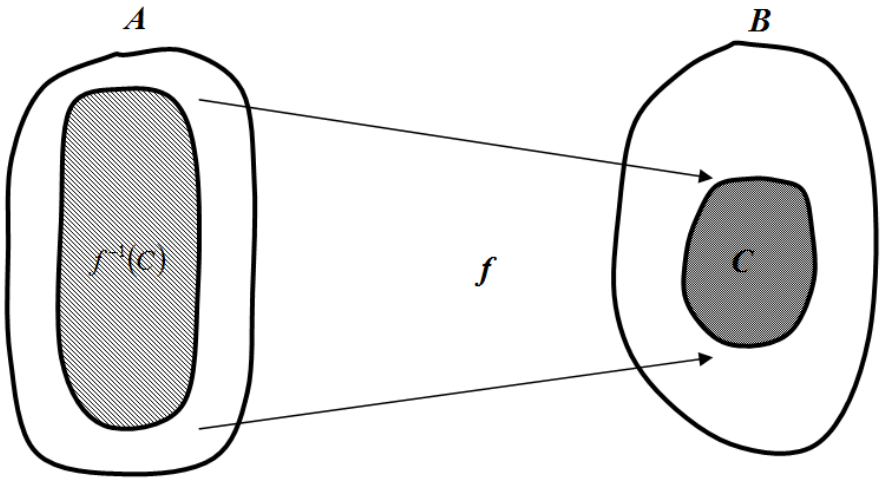

Рис. 6. Діаграма прообразу C при відображенні f

Поставимо у відповідність кожній функції $f : A \to B$ відношення еквівалентності на A і позначимо через R_f. Таке відношення ще має назву *ядерного відношення* або *ядра функції f*, і визначимо:

$$R_f = \{\langle x, y\rangle : x \in A \text{ і } y \in A \text{ і } f(x) = f(y)\},$$
$$\text{або } xR_f y \text{, якщо і тільки, коли } f(x) = f(y). \tag{3}$$

Тоді діаграма бути мати вигляд, наведений на рис. 7, де $p_1(\langle x, y\rangle) = x$ і $p_2(\langle x, y\rangle) = y$ декартов квадрат, тобто R_f отримується підйомом f вдовж самого себе.

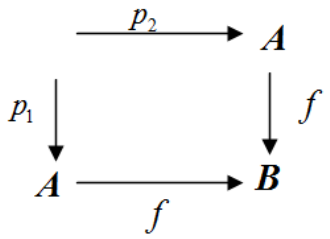

Рис. 7. Комутативна діаграма епі-моно-розкладання стрілок

На цій основі можна підтвердити лему про квадрати, коли діаграма, яка надана на рис. 8, комутативна, тоді якщо два малих квадрата декартові, то зовнішній прямокутник також декартовий (нижня і верхня сторони якого є композиціями відповідно нижніх і верхніх сторін малих квадратів).

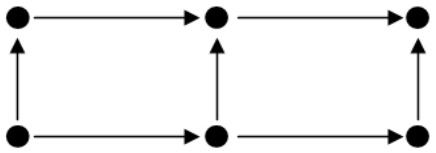

Рис. 8. Комутативна діаграма квадрату

Якщо зовнішній прямокутник і правий квадрат декартові, то декартовий і лівий квадрат. Відповідно, якщо прямокутник перевернути на 90°, то коли зовнішній прямокутник і ніжній квадрат декартові, то верхній квадрат теж декартовий.

У вільній категорії (рис. 9(а)) стрілка $f : a \to b$ мономорфна, тоді і тільки тоді, коли квадрат декартовий; якщо квадрат декартовий (рис. 9(б)), і f — монострілка, то g також мономорфна.

а **б**

Рис. 9. Комутативні діаграми квадратів множин: а – у вільній категорії; б – якщо квадрат декартовий

Поняття амальгами є двійковим по відношенню до поняття зворотного образу.

Амальгамою є пари стрілок $a \overset{f}{\leftarrow} c \overset{g}{\rightarrow} b$ з загальним початком [7], як надано на рис. 10.

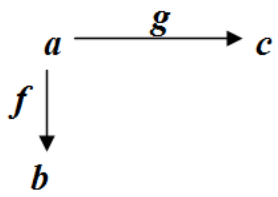

Рис. 10. Діаграма пари стрілок $a \overset{f}{\leftarrow} c \overset{g}{\rightarrow} b$

У категорії **Set** амальгама отримується побудовою диз'юнктивного об'єднання $b+c$ і ототожненням $f(x)$ з $g(x)$ для кожного $x \in a$ (тобто амальгама співпадає з коприрівнювачем пари композицій $a \overset{f}{\rightarrow} b \mapsto b+c$, $a \overset{g}{\rightarrow} c \mapsto b+c$).

Таким чином β може бути повною, якщо у ній діаграма має межу. Двійковим образом категорії β є коповнота, якщо кожна β-діаграма має комежу. А біповною є категорія, яка є одночасно повною і коповною.

Кінцевою може бути діаграма, яка має кінцеву кількість об'єктів і кінцеве число стрілок між ними. Таким чином, категорія може бути кінцево повною, якщо вона має межу будь-якої діаграми. А кінцево коповною може бути діаграма, яка має комежу і є кінцевою. Таким чином і визначається кінцева біповнота.

Для даних множин A і B можна утворити у **Set** сукупність B^A усіх функцій, визначених на A, які приймають значення B, тобто:

$$B^A = \{f : f - \text{функція із } A \text{ у } B\}. \qquad (4)$$

Щоб визначити B^A у стрілках необхідно асоціювати з множиною B^A спеціальну стрілку

$$ev : B^A \times A \to B. \qquad (5)$$

Категорний опис B^A базується на тому факті, що спеціальна стрілка має властивості універсальності серед усіх функцій вигляду $C \times A \overset{g}{\rightarrow} B$.

Для будь-якої такої функції g існує одна і тільки одна функція $\hat{g} : C \to B^A$, для якої діаграма, яка надана на рис. 11, є комутативною.

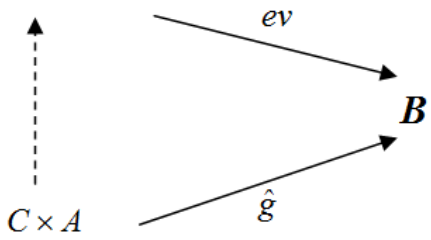

Рис. 11. Комутативна діаграма функторного добутку функцій

На діаграмі на парі $\langle c,a\rangle \in C\times A$ значення функції дорівнює:

$$\hat{g}\times id_A = \langle \hat{g}(c), id_A(a)\rangle = \langle \hat{g}(c), a\rangle . \qquad (6)$$

Таке визначення функції $\hat{g}$ зумовлено тою обставиною, що при кожному фіксованому c функція g визначає відображення $A\to B$, яке отримується, якщо перший елемент упорядкованих пар, які є аргументом функції g, покласти рівним c, у той-же час, як другий буде пробігати множину A. Іншою мовою, для цього $c\in C$ визначається $g_c : A\to B$ правилом $g_c(a) = g(\langle c,a\rangle)$ для кожного $a\in A$.

Функція $\hat{g}$ визначається рівнянням $\hat{g}(c) = g_c$ для $c\in C$. Для вільної пари $\langle c,a\rangle \in C\times A$ справедливим є рівняння:

$$ev(\langle \hat{g}(c), a\rangle) = g_c(a) = g(\langle c,a\rangle). \qquad (7)$$

Вимога комутативності діаграми, яка наведена на рис. 11, тобто правильності рівняння (7) означає, що $\hat{g}(c)$ повинна бути функцією, яка для цього a дає $g(\langle c,a\rangle)$, тобто $\hat{g}(c)$ повинна співпадати з визначеної вище g_c.

Якщо множина A є підмножиною множини B, то функція включення $A\mapsto B$ ін'єктивна і тому мономорфна. З іншого боку, вільна мономорфна функція $f : C\mapsto B$ визначає підмножину множини B, при якій $\mathrm{Im}\, f = \{f(x) : x\in C\}$ (рис. 12). Тобто, f індуцирує бієкцію між C та $\mathrm{Im}\, f$. Далі отримуємо $C\cong \mathrm{Im}\, f$.

Таким чином, область визначення мономорфної функції ізоморфна деякій підмножині області значень цієї функції. Іншою мовою, область визначення є, з точністю до ізоморфізма, підмножиною області значень.

Підмножиною або підоб'єктом β-об'єкта d або підоб'єктом у d є мономорфна β-стрілка $f : a\mapsto d$ з кінцем d.

Якщо D — довільна множина, то множина усіх підмножин $\mathrm{P}(D)$ є *множиною-степеню* множини D.

Таким чином, $\mathrm{P}(D) = \{A : A \text{ підмножина множини } D\}$.

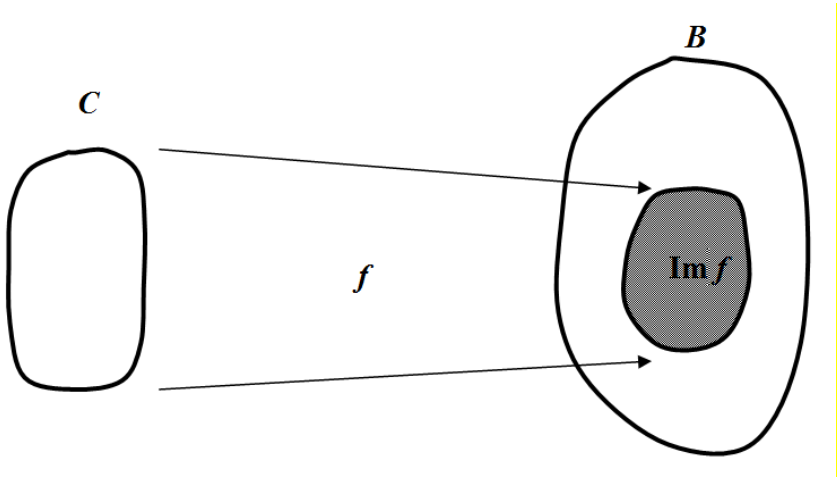

Рис. 12. Діаграма $f : C\mapsto B$, при якій $\mathrm{Im}\, f = \{f(x) : x\in C\}$

Відношення теоретико-множинного включення є частковим порядком на множині-степені $\mathrm{P}(D)$, тобто пара $(\mathrm{P}(D),\subseteq)$ утворює частково-упорядочену множину, яку можна уявляти як категорію, у якій стрілка $A \to B$ мається тільки тоді, коли $A \subseteq B$. При наявності стрілки $A \to B$ діаграма, яка надана на рис. 13(а), комутативна.

а **б**

Рис. 13. Комутативні діаграми: а – при $A \subseteq B$, $A \subseteq B, D$; б – при $f : a \mapsto d$, $g : b \mapsto d$, $h : a \to b$

Це підказує визначення відношення включення між підоб'єктами об'єкта *d*. Для заданих підоб'єктів $f : a \mapsto d$ і $g : b \mapsto d$ покладемо $f \subseteq g$ тоді і тільки тоді, коли існує β-стрілка $h : a \to b$, при якій діаграма, яка наведена на рис. 13(б), комутативна, тобто $f = g^{\circ}h$. Така стрілка *h* буде мономорфною, тобто буде підоб'єктом об'єкта *b*, що посилює аналогію з теоретико-множинним випадком. Таким чином, $f \subseteq g$ тоді і тільки тоді, коли *f* проходить через *g*.

Поняття включення на підоб'єктах підмножин можна розглядати наступним чином:

Відношення рефлективності при $f \subseteq f$, так як $f = f \circ 1_a$ (рис. 14).

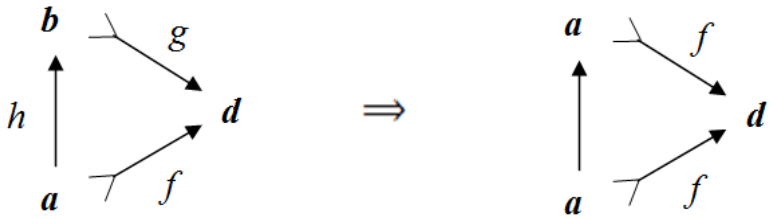

Рис. 14. Комутативні діаграми рефлективності

Відношення транзитивності: якщо $f \subseteq g$ і $g \subseteq f$, то $f \subseteq k$, так як з $f = g \circ h$ і $g = k \circ i$ виходить $f = k \circ (i \circ h)$ (рис. 15).

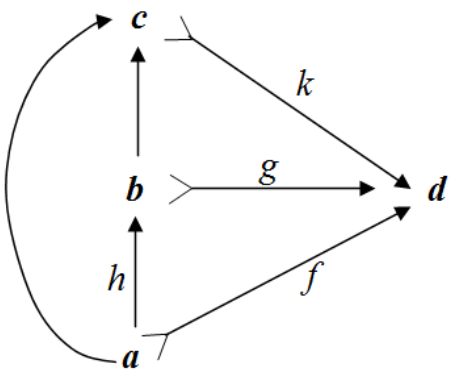

Рис. 15. Комутативна діаграма транзитивності

Якщо $f \subseteq g$ і $g \subseteq f$, то f і g пропускається друг через друга, як надано на рис. 16, то $f = g \circ h$, $g = f \circ i$.

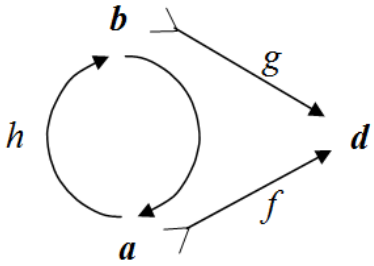

Рис. 16. Діаграма тотожності підмножин при $f \subseteq g$ і $g \subseteq f$

У цьому випадку $h : a \to b$ буде ізострілкою, а i — зворотною до неї. Таким чином, якщо $f \subseteq g$ і $g \subseteq f$, то стрілки f і g мають ізоморфні початки. Тому їх ще називають *ізоморфними підоб'єктами* ($f \cong g$). Відношення ізоморфності є відношенням еквівалентності. Кожна стрілка $f : a \mapsto d$ визначає клас еквівалентності:

$$[f] = \{g : f \cong g\}. \tag{8}$$

При цьому утворюється множина:

$$Sub(d) = \{[f] : f \text{ є 1 монострілкою і } cod\ f = d\}.$$

Тобто, елементи множини $Sub(d)$ є підоб'єктами. Тому підоб'єктами об'єкту d вважаються класи еквівалентності монострілок з кінцем у d.

Для визначення відношення включення на введених об'єктах, визначимо $[f] \subseteq [g] \Rightarrow f \subseteq g$.

Для визначення залежності класів еквівалентності від самих множин та підмножин розглянемо наступне твердження: якщо $[f]=[f']$ і $[g]=[g']$, то $f \subseteq g$, при $f' \subseteq g'$. Тобто відношення тотожності стійке відносно ізоморфності підоб'єктів.

Підоб'єкти об'єкту d утворюють частково упорядковану множину $(Sub(d),\subseteq)$. Дійсно, якщо $[f]\subseteq[g]$ і $[g]\subseteq[f]$, то $f \subseteq g$ і $g \subseteq f$, відповідно $f \cong g$, з чого витікає, що $[f]=[g]$.

В подальшому вираз $f \cong g$ буде використовуватися, коли вважається, що f і g є одним і тим же підоб'єктом, а вираз $f = g$ буде визначати, що f і g у дійсності є однією і тою ж стрілкою.

Висновки

Описуючи категорію підмножин, необхідно повернутися до поняття елементів множин. Елемент x множини $A(x \in A)$ можна ототожнити з одноелементною підмножиною $\{x\}$ множини A і, відповідно, зі стрілкою $\{x\}\mapsto A$ з кінцевого об'єкта $\{x\}$ у A. Зворотно функція $f:1\to A$ визначає у категорії **Set** елемент з A, а саме f-образ єдиного елементу кінцевого об'єкта 1. Якщо категорія β має кінцевий об'єкт 1, то елементом β-об'єкта a є будь-яка β-стрілка $x:1\to a$. При цьому $x:1\to a$ завжди буде моно стрілкою.

У подальшому виникає питання про властивості елементів у **Set.** Чи повинен будь-який об'єкт, який є не початковим, мати елементи? Чи можливо охарактеризувати мономорфні і епіморфні стрілки у термінах елементів їх початку і кінця? Усі ці питання необхідно розглядати у комплексі, розкриваючи імена стрілок та визначаючи класифікацію підоб'єктів, з метою подальшого розкриття питань взаємодії множин та підмножин загрозливих впливів на об'єкти та підоб'єкти множин механізмів захисту інформації [8].

Список літератури

1. Бірюков, В.О. Композиція і категорії функцій систем загроз в областях систем захисту інформації / В.О. Бірюков, І.М. Павлов // Захист інформації. – 2013. – № 1. – 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. — 2013. — № 1. — С. 36–45.
3. Павлов, І.М. Проектування комплексних систем захисту інформації [Текст] : підруч. для студ. вищ. навч. закл., які навчаються за галуззю знань «Інформаційна безпека» / І.М. Павлов, В.О. Хорошко ; Держ. служба спец. зв'язку та захисту інформації, Військ. ін-т телекомунікацій та інформатизації Нац. техн. ун-ту України «Київ. політехн. ін-т», Держ. ун-т інформ.-комунікац. технологій. — К. : ВІТІ : ДУІКТ, 2011. — 244 с.
4. Manes, E.G. Category Theory Applied to Computation and Control / E.G. Manes // Proceedings of the 1st International symposium, San Francisco, February 25–26, 1974. Edited by E.G. Manes. — Berlin : Springer-Verlag, 1975. — 245 p.
5. Попов, М.М. Аксіоматична теорія множин. Частина І: Система аксіом ZFC і вступ до теорії моделей / М.М. Попов ; Чернівецький національний університет імені Юрія Федьковича. — Чернівці, 2011. — 79 с.
6. Grayson, R. Heyting-valued models for intuitionistic set theory / R. Grayson // Lecture Notes in Mathematics. — 1979. — Vol. 753. — PP. 402–414.
7. Плоткин, Б.И. Универсальная алгебра, алгебраическая логика и базы данных : монография / Б.И. Плоткин. — М. : Наука, 1991. — 446 с.
8. Павлов, И.Н. Формальное описание процесса проектирования комплексных систем защиты информации в информационно-телекоммуникационных системах [Текст] / И.Н. Павлов, Г.Д. Радзивилов // Вісник ДУІКТ. — К. : 2010. — Т. 8, № 1. — С. 84–93.

АМАЛЬГАМЫ, ПОЛНОТА ДИАГРАММ И ПОДОБЪЕКТОВ МНОЖЕСТВ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

И.Н. Павлов

Национальный технический университет Украины «Киевский политехнический институт»,
просп. Победы, 37, Киев, 03056, Украина; e-mail: pavlov@ukr.net

В статье рассматриваются математические модели отношений множеств и подмножеств на основе анализа категорий логики с целью дальнейшего проведения анализа угроз на системы защиты информации. Приведено описание обратного образа, ядерных отношений и амальгам в множествах систем защиты информации.
Ключевые слова: амальгамы, множества, подмножества, объекты, подобъекты, функции, система защиты информации

AMALGAMS, COMPLETENESS OF DIAGRAMS AND SUB-OBJECTS OF SETS IN INFORMATION SECURITY SYSTEMS

Igor M. Pavlov

National Technical University of Ukraine «Kyiv Polytechnic Institute»,
37 Peremogy Ave., Kyiv, 03056, Ukraine; e-mail: pavlov@ukr.net

This paper focuses on mathematical models of the relationship between sets and subsets based on analysis of the logic categories for further analyze threatening impacts on information security systems. The description of the pullback, nuclear relations and amalgams in the sets of information security systems are given.
Keywords: amalgams, sets, subsets, objects, sub-objects, functions, information security system