УДК 004.415.056.5(075)

І.М. Павлов,
кандидат технічних наук,
доцент

МОРФІЗМ ФУНКЦІЙ І БІЄКТИВНІСТЬ ОБ'ЄКТІВ ПРИ ПРОЕКЦІЇ МНОЖИН ЗАГРОЗ ТА ОБЛАСТЕЙ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

У статті розглядаються основні підходи до визначення математичного апарату категорійного аналізу логіки взаємовідносин загроз та областей системи захисту інформації під час ескізного проектування систем захисту інформації.

Ключові слова: *композиція, категорії, множина, підмножина, об'єкт, функції та система захисту інформації.*

В статье рассматриваются основные подходы по определению математического аппарата категорийного анализа логики взаимоотношений угроз и областей системы защиты информации при эскизном проектировании систем защиты информации.

Ключевые слова: *композиция, категории, множества, подмножества, объект, функции и система защиты информации.*

This article deals with the main approaches to the definition of the mathematical apparatus of categorical analysis of logical relationships threats and areas of information security system for the schematic design of information security.

Keywords: *composition, categories, sets, subsets, object, functions and information security system.*

Під час ескізного проектування систем захисту інформації необхідно формалізувати поняття безлічі загроз та механізмів захисту систем захисту інформації, їх взаємовідносини. Необхідно розкривати поняття, які необхідні для пояснення математичних взаємовідносин множин між собою. Запропонований в [1] категорійний апарат теорії множин дозволяє пояснити математичні моделі, які повинні використовуватися під час ескізного проектування систем захисту інформації. Це важливо, оскільки мало наукових робіт, які б пояснювали процес перетворення загрозливої інформації в небезпеку для систем захисту інформації, що є критичним для захисту інформації. Відомо, що система захисту повинна блокувати загрози для інформаційних систем, але часто не береться до уваги, що існує безліч загроз для самих систем захисту інформації. Тому необхідно захищати і самі системи захисту інформації. І на етапі ескізного проектування необхідно розглядати вплив таких загроз на системи захисту інформації. Множини цих загроз є небезпечними і в цій статті розкриваються математичні відношення між множинами небезпечних загроз і множинами систем захисту інформації.

У зв'язку з цим, виникає об'єктивна необхідність подальшого визначення основних математичних підходів у вивченні процесів, які виникають в системах

захисту інформації під час впливу небезпечних для цих множин загроз. Для цього необхідно визначити категорійний апарат та сформулювати основні математичні підходи до проведення аналізу процесів взаємодії загроз и системи захисту інформації. Основою для проведення цього аналізу є модель процесу захисту інформації з повним перекриттям загроз з використанням теорії інформації та теорії топосів.

Представимо b – об'єкт деякої категорії β – множин загроз або множин областей системи захисту інформації. Тоді β – функція (стрілка) 1_b визначається однозначно в силу її властивості, яке означено законом тотожності [2].

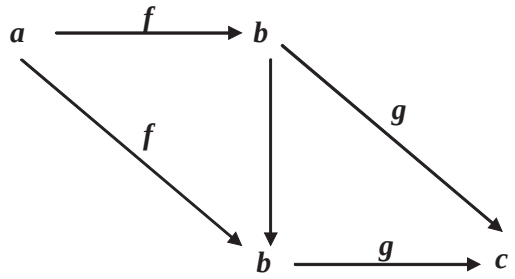

Рис. 1. Тотожна діаграма взаємозв'язків двох функцій множин загроз та системи захисту

Тобто, коли стрілка $1'$: $b \to b$ має такі властивості, що і діаграма (рис. 1), комутативна для будь-яких β-стрілок f та g вказаного вигляду, то у приватному випадку, коли $f = 1'$ та $g = 1_b$, комутативна діаграма представлена на рис. 2.

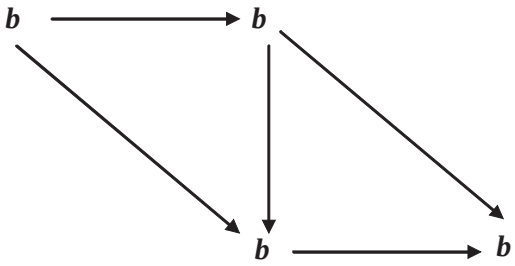

Рис. 2. Комутативна діаграма дискретних категорій функцій множини

Як наглядно бачимо, $1_b = 1_b \circ 1'$ правий трикутник. За законом тотожності (для $f = 1'$) $1_b \circ 1' = 1'$. Тобто $1_b = 1'$.

Оскільки одинична стрілка 1_b визначається однозначно за об'єктом b, то на практиці ототожнюється об'єкт b з функцією (стрілкою) 1_b: b: $b \to b$, $b \circ f$ і т.п.

Згідно аксіом категорій [3], сукупність β-стрілок включає одиничну стрілку для кожного β-об'єкта. Категорія β є дискретною, коли у ній виконується наступна умова: кожна стрілка (функція) є одиничною для деякого об'єкта. Дискретна категорія являє собою приклад категорії передпорядку. Тобто дискретна категорія є сукупністю об'єктів. Будь-яка множина X може стати дискретною категорією, коли добавляються одиничні стрілки $x \to x$ для кожного $x \in X$, тобто X перетворюється у категорію передпорядку, яка відповідає відношенню $R \subseteq X \times X$, такому, що xRy тоді і тільки тоді, коли $x = y$.

Категорія B (рис. 2) є моноїдом, оскільки згідно з [4] моноїд це:

$$\mathbf{M} = (M, *, e). \qquad (1)$$

де, M – деяка множина;

* – бінарна операція на M, тобто функція з $M \times M$ у **M**, яка ставить у відповідність кожній парі $\langle x, y \rangle \in M \times M$ елемент $x * y$ з M, яка асоціативна, тобто $x * (y * z) = (x * y) * z$ для будь-яких $x, y, z \in M$;

E – елемент множини M, яка є одиницею моноїду, для якого $e * x = x * e = x$ при усіх $x \in M$.

По будь-якому моноїду **M** будується категорія з одним об'єктом (рис. 3):

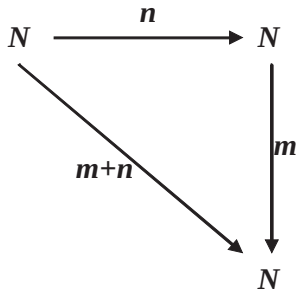

Рис. 3. Комутативна діаграма побудови моноїду

У якості об'єкта береться множина M, а в якості функцій (стрілок) M→M – елементи з M, крім того вважається, що e = 1_M. Композиція стрілок x, $y \in M$ задається за правилом: $x \circ y = x * y$. Коли β – категорія з єдиним об'єктом a, а сукупність M – сукупність її стрілок, то трійка $(M, \circ, 1_a)$ є моноїдом.

Введемо поняття **Set**$^{\rightarrow}$, де **Set** – усі множини зі своїми функціями.

Об'єктами категорії функцій **Set**$^{\rightarrow}$ є усі функції $f : A \to B$. Функція з **Set**$^{\rightarrow}$ об'єкта $f : A \to B$ до **Set**$^{\rightarrow}$ об'єкта $g : C \to D$ являє собою пару функцій $\langle h, k \rangle$, як наведено на діаграмі представлені на рис. 4.

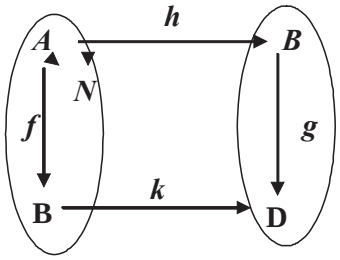

Рис. 4. Комутативна діаграма побудови функцій **Set**$^{\rightarrow}$

Діаграма, яка надана на рис. 4, комутативна, тобто $g \circ h = k \circ f$.

Якщо композицію задати правилом $\langle j, l \rangle \circ \langle h, k \rangle = \langle j \circ h, l \circ k \rangle$. Коректність правила можна представити на рис. 5.

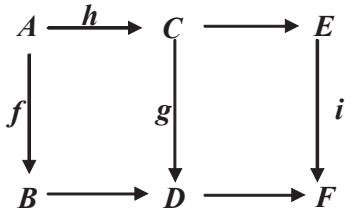

Рис. 5. Комутативна діаграма функцій **Set**$^{\rightarrow}$ за правилом $\langle j, l \rangle \circ \langle h, k \rangle = \langle j \circ h, l \circ k \rangle$.

Відносні категорії розглянемо як спеціалізацію функцій, коли функції (стрілки) мають фіксовані кінець та початок.

Розглянемо множину чисел **R**, в якій визначається категорія функцій **Set** $\downarrow$ **R**, її об'єктами є функції $f : A \to R$ з областю значень *R*. У якості функцій з $f : A \to R$ у $g : B \to R$ беруться функції $k : A \to B$ для яких комутативний трикутник, представлений на рис. 6.

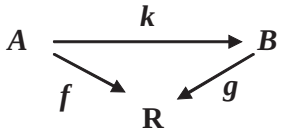

Рис. 6. Комутативна діаграма побудови відносної категорії функцій

Об'єкти категорії **Set** $\downarrow$ **R** можна уявити у вигляді пар (A, f) для $f : A \to R$. Тоді композиція функцій має вигляд:

$$(A, f) \xrightarrow{k} (B, g) \xrightarrow{l} (C, h). \qquad (2)$$

У цій множині визначається діаграма, наведена на рис. 7.

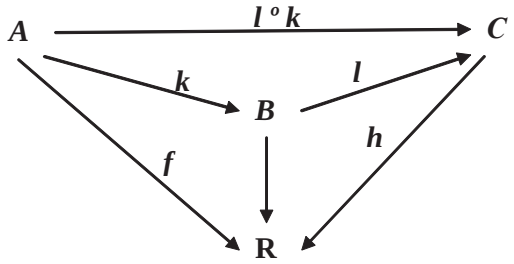

Рис. 7. Комутативна діаграма побудови відносної категорії функцій з підкатегорією множини *R*

У **Set** $\downarrow$ **R** визначається як функція $l \circ k : (A, f) \to (C, h)$.

Аналогічно для будь-якої множини *X* можна визначити категорію **Set** $\downarrow$ **X** функцій із значеннями у *X*. У загальній ситуації, коли **β** – деяка категорія, а *a* – будь-який її об'єкт, тоді об'єктами категорії в $\downarrow a$ об'єктів над *a* є усі **β**-стрілки з кінцем у об'єкті *a*, а стрілками з $f : b \to a$ до $g : c \to a$ такі **β**-стрілки $k : b \to c$, що трикутник, представлений на рис. 8а комутативний, тобто $g \circ k = f$.

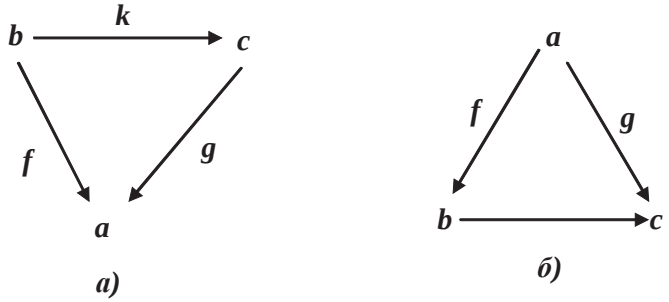

Рис. 8. Комутативна діаграма побудови:
а) категорії в $\downarrow a$; б) категорії в $\uparrow a$

Категорії типу, наведеного на рис. 8б, визначаються як категорії в $\uparrow a$ об'єктів під a, об'єктами якої є усі **β**-стрілки з початком a, а стрілками з $f : a \to b$ до $g : a \to c$ такі **β**-стрілки $k : b \to c$, що трикутник комутативний, тобто $k \circ f = g$. На рис. 8а,б представлені відносні категорії функцій множин.

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

Якщо визначити, що $f : A \to B$ ін'єктивна (рис. 9).

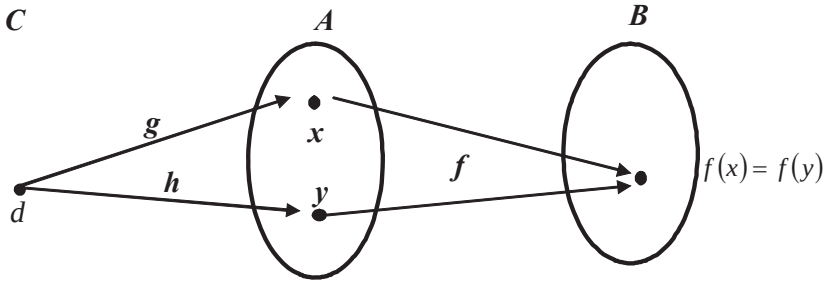

Рис. 9. Модель побудови ін'єктивної функції або мономорфної стрілки

Стрілки $g, h : C \to A$ є мономорфними або монострілками. Це твердження також правильне для $f : A \to B$. За умовою, коли функція $g(x) = f(x)$ або $h(y) = f(y)$, то функції $g, h, f : C \to B$ є ін'єктивні. Тобто правильний запис:

$$q, h : C \rightarrowtail A \Rightarrow f : A \rightarrowtail B \qquad 3)$$

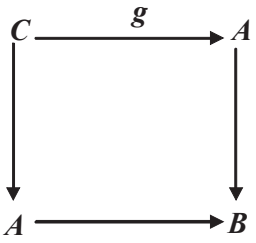

Рис. 10. Комутативна діаграма ін'єктивної функції $g, h : C \rightrightarrows A, f : A \rightrightarrows B$

Теоретико-множинна функція $f : A \to B$ сур'єктивна або є накладенням, коли її область значень B співпадає з множиною усіх її значень, тобто для кожного $y \in B$ існує деякий $x \in A$, такий, що $y = f(x)$. Іншою мовою, кожен елемент з B з'являється у якості виходу f. Тобто вільний елемент $b \in B$ є *образом* f (a) деякого елементу $a \in A$, або $f : a \twoheadrightarrow b$.

У цьому випадку функція $f : A \to B$ є ін'єктивною та суб'єктивною – бієктивною. Тобто $f : a \twoheadrightarrow B$. і перехід з A до B за допомогою f може бути обернений.

Ін'єктивність та суб'єктивність функцій можна представити як ідентифікацію та аутентифікацію загроз в областях системи захисту.

Бієктивну функцію $f : A \to B$ можна представити як:

$$g \circ f = \mathbf{id}_A \text{ та } f \circ g = \mathbf{id}_B. \quad (4)$$

Так як $f : A \to B$ бієктивна, то взаємовідношення множин та підмножин *ізоморфно*, тобто $A \cong B$. За приклад (рис. 9) візьмемо вільну множину A, тоді:

$$B = A \times \{d\} = \{\langle x, d\rangle : x \in A\}. \quad (5)$$

Фактично B є множина A з міткою d, яка закріплена до кожного її елемента. Правило $f(x) = \langle x, d\rangle$ задає бієкцію $f : A \to B$, яка встановлює $A \cong B$. У топології такі ізоморфні відносини ще мають назву гемеоморфними, оскільки існує безперервна бієкція, для якої зворотне відображення також безперервно.

Якщо Σ – пропозиція категорної мови, то для об'єктів множин існує двійкова пропозиція категорної мови – $\Sigma^{\text{ДВ}}$. Для категорії $\boldsymbol{\beta}$ двійкова категорія $\beta^{\text{ДВ}}$ будується таким чином.

Категорії $\boldsymbol{\beta}$ та $\beta^{\text{ДВ}}$ мають теж самі об'єкти. Для кожної $\boldsymbol{\beta}$-стрілки $f : a \to b$ мається $\boldsymbol{\beta}$-стрілка $f^{\text{ДВ}} : b \to a$ (особисту для кожної f). Так отримані стрілки вичерпують усі стрілки категорії $\beta^{\text{ДВ}}$. Композиція $f^{\text{ДВ}} \circ g^{\text{ДВ}}$ визначена тоді і тільки тоді, коли у $\boldsymbol{\beta}$ визначена композиція $g \circ f$ та $f^{\text{ДВ}} \circ g^{\text{ДВ}} = (g \circ f)^{\text{ДВ}}$ (рис. 11).

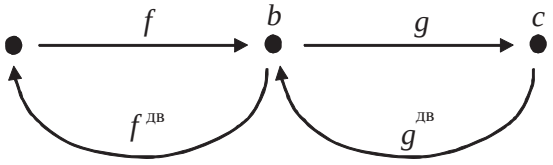

Рис. 11. Композиція двійкових категорій об'єктів

При цьому $\text{dom } f^{\text{ДВ}} = \text{cod } f$ та $\text{cod } f^{\text{ДВ}} = \text{dom } f$.

Якщо уявити множини A та B як добуток множин $A \times B$, тоді згідно з рис. 9, маємо:

$$A \times B = \{\langle x, y\rangle : x \in A, y \in B\}. \quad (6)$$

Згідно з теорією проекцій отримуємо відображення:

$$v_A : A \times B \to A, v_B : A \times B \to B, \quad (7)$$

які задаються рівняннями:

$$v_A(\langle x, y\rangle) = x, v_B(\langle x, y\rangle) = y. \quad (8)$$

Якщо задана ще множина C з парою відображень $f : C \to A, g : C \to B,$ то визначається відображення $v : C \to A \times B$ з правилом $v(x) = \langle f(x), g(x)\rangle,$ яке у вигляді діаграми представлено на рис. 12.

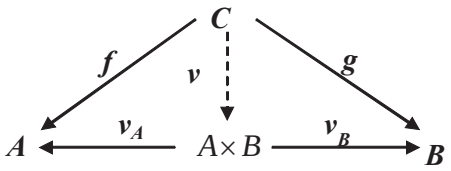

Рис. 12. Комутативна діаграма відображень множин $v : C \to A \times B$

Тоді $v_A(p(x)) = f(x), v_B(p(x)) = g(x)$ для кожного $x \in C$. Таким чином, $v_A \circ v = f, v_B \circ v = g$, тобто приведена на рис. 12 діаграма комутативна. Більш того, v є єдиною стрілкою, для якої діаграма комутативна. Дійсно, якщо $v(x) = \langle y, z \rangle$, то за умовою $v_A \circ v = f$ буде $v_A(v(x)) = f(x)$, тобто $y = f(x)$. Аналогічно, якщо $v_B \circ v = g$, тоді $z = g(x)$.

Добуток у категорії β двох об'єктів a і b представимо через $a \times b$, сумісно з парою $(dob_a : a \times b \to a, dob_b : a \times b \to b)$ **β**-стрілок, так, що для деякої пари $\langle f : c \to a, g : c \to b \rangle$ β-стрілок існує одна і тільки одна стрілка $\langle f, g \rangle : c \to a \times b$, для якої діаграма має вигляд, представлений на рис. 13.

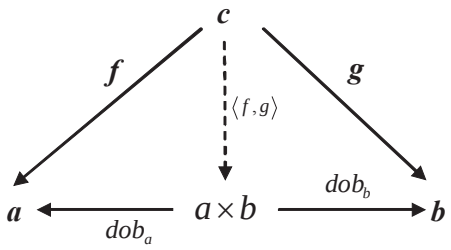

Рис. 13. Комутативна діаграма добутку ізоморфних множин $dob : c \to a \times b$

Діаграма комутативна, так як $dob_a \circ \langle f, g \rangle = f, dob_b \circ \langle f, g \rangle = g$. Якщо розглянути рис. 12, 13, то $dob_a, dob_b = v_a, v_b = pr_a, pr_b$ – проекції двох об'єктів. Якщо **β**-об'єкт d сумісний з парою $p : d \to a$ і $g : d \to b$ задовольняє рис. 12, 13, то розглянемо діаграму, наведену на рис. 14.

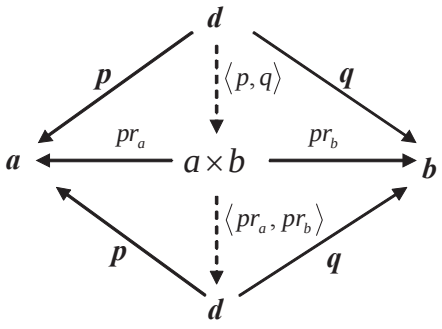

Рис. 14. Комутативна діаграма проекції ізоморфних підмножин $pr_a : d \to a, pr_b : d \to b$

При цих проекціях $pr_a : a \times b \to a, pr_b : a \times b \to b$ стрілка $\langle p, q \rangle$ однозначно визначена. Стрілка $\langle pr_a, pr_b \rangle$ також є однозначно визначеним добутком pr_a, pr_b стрілок відносно $p : d \to a, q : d \to b$. Оскільки d є добутком об'єктів a, b, то існує тільки одна стрілка $s : d \to d$ для якої правильна діаграма, яка наведена на рис. 15.

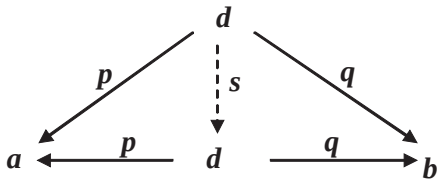

Рис. 15. Комутативна діаграма тотожності ізоморфних підмножин

При $s = 1_d$ ця діаграма комутативна. У той же час, як відомо з комутативності діаграми, яка наведена на рис. 14, при $s = \langle pr_a, pr_b \rangle \circ \langle p, q \rangle$ діаграма, представлена на рис. 15 також комутативна, тобто $p \circ \langle pr_a, pr_b \rangle \circ \langle p, q \rangle = pr_a \circ \langle p, q \rangle = p$ і т.п. З цього можна виразити, що:

$$\langle pr_a, pr_b \rangle \circ \langle p, q \rangle = 1_d. \qquad (9)$$

Міняючи ролями d і $a \times b$ можна прийти до рівності $\langle p, q \rangle \circ \langle pr_a, pr_b \rangle = 1_{a \times b}$. Таким чином, $\langle p, q \rangle : d \cong a \times b$. Композиція ізострілки $\langle p, q \rangle$ з проекціями для $a \times b$ дає проекції для d, як видно з рис. 15. Тобто $\langle p, q \rangle$ є єдиною стрілкою $d \to a \times b$.

Приклади комутативних діаграм тождественних ізоморфних підмножин представлені на рис. 16.

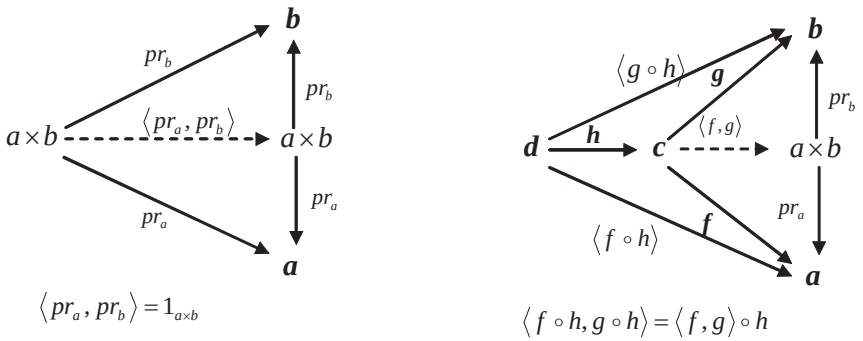

Рис. 16. Приклади комутативних діаграм тотожних ізоморфних підмножин при:
$\langle pr_a, pr_b \rangle = 1_{a \times b}$, $\langle f \circ h, g \circ h \rangle = \langle f, g \rangle \circ h$

Розглянуті стандартні теоретико-множинні конструкції дозволяють представити взаємовідносини різних множин та підмножин, які є 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 [6].

У подальшому будуть розглянуті поняття граничності, які охоплюють усі побудови в тих або інших категоріях множин та підмножин. Це важливо для з'ясування функторних відображень добутків об'єктів, кінцевості добутків та контрдобутків множин та підмножин.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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

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

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

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

6. *Кобозева А.А.* Аналіз захищеності інформаційних систем / А.А. Кобозева, І.О. Мачалін, В.О. Хорошко. – Київ. Вид. ДУІКТ. – 2010. – 316 с.

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

Отримано 30.08.2013