УДК 004.415.056.5(075)

МАТЕМАТИЧНА МОДЕЛЬ ПРОЕКТНИХ ВІДНОСИН ЗАГРОЗ ТА МНОЖИН СИСТЕМИ ЗАХИСТУІНФОРМАЦІЙНОЇ МЕРЕЖІ

DOI 10.36994 / 2788-5518-2022-01-03-14

Толюпа С.В., *д.т.н., проф. Київський національний університет імені Тараса Шевченка, Київ, Україна. tolupa@i.ua*

Лукова-Чуйко Н.В., *д.т.н., проф. Київський національний університет імені Тараса Шевченка, Київ, Україна. lukova@ukr.net*

Бучик С.С. *, д.т.н., проф. Київський національний університет імені Тараса Шевченка, Київ, Україна. s_stbu@ukr.net*

Штаненко С.С.*, к.т.н., доц. Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна. sh_sergei@ukr.net*

Анотація: *Результативне рішення задач аналізу і синтезу систем управління інформаційною безпекою не може бути забезпечено одними лише способами простого опису їх поведінки в різних умовах – системотехніка видвигає проблеми, які потребують кількісні оцінки характеристик. На сьогоднішній момент створення систем управління інформаційною безпекою не можливе без дослідження й узагальнення світового досвіду побудови інформаційних систем та їх складових підсистем, одними з ключових яких є системи захисту інформації та протидії вторгненням в інформаційну систему. Складовими математичного забезпечення таких систем є моделі процесів нападу на механізми захисту та блокування або знищення самих кіберзагроз. Базою таких моделей є математичний апарат, який повинен Dr. habil, Prof. забезпечити адекватність моделювання процесів захисту інформації для будь-яких умов впливу кіберзагроз. При визначенні математичного апарату необхідно чітко розуміти як будуються ті або інші множини кіберзагроз, та як здійснюються взаємовідносини самих множин кіберзагроз, множин елементів системи захисту та множин систем виявлення кібератак, які повинні контролювати правильність роботи процесу захисту інформації. У статті аналізуються різні варіанти побудови моделей системи управління інформаційною безпекою та створена математична модель, яка враховує внутрішні взаємозв'язки різних підмножин складових системи захисту інформації під час впливу кіберзагроз.*

Ключові слова: *граф, діаграми, кіберзагрози, множини, моделі, функції, підмножини, проектування, система захисту інформації, управління інформаційною безпекою*

MATHEMATICAL MODEL OF PROJECT RELATIONS OF THREATS AND SETS OF PROTECTION SYSTEM INFORMATION NETWORK

Serhii Toliupa, *Dr. habil, Prof. Taras Shevchenko National University of Kyiv Kyiv, Ukraine. tolupa@i.ua*

Nataliia Lukova-Chuiko, *Dr.habil,Prof. Taras Shevchenko National University of Kyiv Kyiv, Ukraine. lukova@ukr.net*

Serhii Buchic , *Dr. habil, Prof. Taras Shevchenko National University of Kyiv Kyiv, Ukraine. s_stbu@ukr.net*

Serhii Shtanenko, *Ph.D, Ass. Prof. Heroes of Kruty Military Institute of Telecommunications and Informatization, Kyiv, Ukraine. sh_sergei@ukr.net*

Abstract: *An effective solution to the problems of analysis and synthesis of information security management systems can not be provided by simple ways of simply describing their behavior in different conditions - systems engineering solves problems that require quantitative evaluation of characteristics. Such data, obtained experimentally or by mathematical modeling, should reveal the properties of information security management systems. The main one is efficiency, which means the degree of compliance of the results of information protection to the goal. The latter, depending on the resources available, the knowledge of developers and other factors, can be achieved to one degree or another, and there are alternative ways to implement it. In a number of publications the authors propose the basics of the categorical apparatus of set theory, which allows to explain the relationship between sets of threats and sets of information protection system, which allows to build different mathematical models to analyze information exchange systems in critical application systems. At present, the creation of information security management systems is not possible without research and generalization of world experience in building information systems and their constituent subsystems, one of the key of which are information protection and intrusion prevention systems. Components of the process of attacking the mechanisms of protection and blocking or destruction of cyber threats themselves are components of the mathematical support of such systems. The basis of such models is the mathematical apparatus, which should ensure the adequacy of modeling of information security processes for any conditions of cyber threats. When defining the mathematical apparatus, it is necessary to*

clearly understand how certain sets of cyber threats are built, and how the sets of cyber threat sets, sets of security system elements and sets of cyber attack detection systems, which should control the correctness of the information security process. The article analyzes various options for building models of information security management system and creates a mathematical model that takes into account the internal relationships of different subsets of components of the information security system under the influence of cyber threats.

Key words: *graph, diagrams, cyber threats, sets, models, functions, subsets, design, information security system, information security management.*

Вступ

Процес розвитку та впровадження новітніх інформаційних технологій забезпечують безпрецедентні умови для накопичення і використання інформації, а також створюють фундаментальну залежність від їх нормального функціонування всіх сфер життєдіяльності суспільства та держави: економіки, політики, сфери національної та міжнародної безпеки тощо. Така залежність стає вразливим місцем у функціонуванні систем і об'єктів критичних національних інфраструктур і дає можливість негативно налаштованим елементам і угрупованням скористатися нею для реалізації протиправних дій у кіберпросторі шляхом порушення цілісності, доступності й конфіденційності інформації та нанесення шкоди інформаційним ресурсам і інформаційним системам. Експерти передбачають, що в прийдешньому році повністю зміниться структура кібероперацій і те, як вони проводяться.

Масовані кібератаки ініціюють створення спеціальних технічних рішень, засобів та систем протидії. Для виявлення мережевих вторгнень використовуються сучасні методи [1-3], моделі [4-5], засоби [6-9] і комплексні технічні рішення для систем виявлення та запобігання вторгнень [10-13], які можуть залишатись ефективними при появі нових або модифікованих видів кіберзагроз. Але на практиці при появі нових загроз та аномалій, породжених атакуючими діями з невстановленими або нечітко визначеними властивостями, зазначені засоби не завжди залишаються ефективними і вимагають тривалих часових ресурсів для їх відповідної адаптації.

На сьогодні вирішення питань забезпечення безпеки в інформаційних системах (ІС) та управління станом їх захищеності описується в роботах вітчизняних та закордонних дослідників, а саме: Бурячка В.Л., Гнатюка С.О., Корченко О.Г., Кузнецова О.О., Субача І.Ю., Хорошко В.О., Євсеєва С.П., Дудикевича В.Б., Пархуця Л.Т., T. Ptaceka, G. Elmasry, P. Albers, O. Camp та інших.

На сьогоднішній момент створення систем управління інформаційною безпекою не можливе без дослідження й узагальнення світового досвіду побудови інформаційних систем та їх складових підсистем, одними з ключових яких є системи захисту інформації та протидії вторгненням в інформаційну систему. Складовими математичного забезпечення таких систем є моделі процесів нападу на механізми захисту та блокування або знищення самих кіберзагроз. Базою таких моделей є математичний апарат, який повинен забезпечити адекватність моделювання процесів захисту інформації для будь-яких умов впливу кіберзагроз.

При визначенні математичного апарату необхідно чітко розуміти як будуються ті або інші множини кіберзагроз, та як здійснюються взаємовідносини самих множин кіберзагроз, множин елементів системи захисту та множин систем виявлення кібератак, які повинні контролювати правильність роботи процесу захисту інформації. У статті пропонується математичний апарат теорії топосів, який дозволяє на рівні спеціальних категорій будувати моделі для теоретико - множинних конструкцій етапу ескізного проектування систем захисту інформації [14 – 15].

Виконання досліджень

Моделлю для множин процесу захисту інформації з повним перекриттям загроз є структура $\mu = \langle A, R, c \rangle$, яка складається з непустої множини *A* (множини процесу захисту інформації у загальному інформаційному процесі), відношення $R = t \times m \times v; R \subseteq A$ (де t – підмножина кіберзагроз, m – множина механізмів захисту, v – множина областей захисту), та с – конкретного індивіду підмножин *R*, при цьому $c \in A$.

Для формулювання варіантів підходів до створення моделей необхідно ввести обмеження при якому $m \geq 1, v \geq 1,$ при $m = u \times b \times h; m \subseteq R$(де u – уразливості бар'єрів захисту, *b* – бар'єри захисту інформації, *h* – підсистема аналізу кіберзагроз).

Згідно інтерпретації перемінних у моделі $\mu \Longrightarrow x$– вільна функція, яка ставить у відповідність кожному позитивному числу *n* деякий елемент $x(n)$. Це є μ – оцінкою і

представляється у вигляді послідовності $x = \langle\overline{x_1, x_i}\rangle$, *i* – й член, якої, є значенням перемінної v_i, яку дає оцінка *x*.

Покладемо істинність моделі $\mu \vDash \varphi[\overline{x_1, x_m}]$, якщо $\mu \vDash \varphi[y]$ для деякої (еквівалентним чином, для будь-якої) оцінки *y*, такої, що $y_i = x_i$ будь-який раз, коли v_i входить вільно у φ. Ця модель $\mu = \langle A, R, c\rangle$, вимога φ^m (належне для φ число m – кратного добутку), тобто $\varphi^m = \{\langle\overline{x_1, x_m}\rangle : \mu = \varphi[\overline{x_1, x_m}]\}$ уявляє собою множину усіх *m*-послідовностей, на яких у моделі μ виконується вимога φ.

Знати множини φ^m для належних *m* – це знати все про виконання вимог у моделі μ. При цьому правила, які визначають виконання для пропорційних зв'язків, відповідають булевим операціям на підмножинах множини A^m. Так, доповнення до φ^m (тобто множина послідовностей, які не задовольняють φ) є множиною послідовностей, які задовольняють ∼φ, пересічення множин φ^m іншого пересічення множин ψ^m складається з послідовностей, які задовольняють вимозі φ ∧ ψ, таким чином, отримуємо:

$$(\sim\varphi)^m = -\varphi^m, (\varphi \wedge \psi)^m = \varphi^m \cap \psi^m, (\varphi \vee \psi)^m = \varphi^m \cup \psi^m \text{ і т. п} \qquad (1)$$

Тобто, якщо *m* є необхідним для φ і ψ числом, то воно буде необхідним і для φ ∧ ψ.

Розглянемо підоб'єкти і їх характеристичні стрілки:

Замінимо множину φ^m характеристичною функцією $[\![\varphi]\!]^m : A^m \to 2$, де:

$$[\![\varphi]\!]^m(\langle\overline{x_1, x_m}\rangle) = \begin{cases} 1, \text{якщо} \mu \vDash \varphi[\overline{x_1, x_m}], \\ 0, \text{у іншому випадку.} \end{cases} \qquad (2)$$

На основі теореми про істинність (якщо топос ε булев, то $\varepsilon \vDash \alpha \vee \sim \alpha$ для будь – якої пропозиції α), маємо рівняння:

$$[\![\sim\varphi]\!]^m = \neg \circ [\![\varphi]\!]^m,$$

$$[\![\varphi \wedge \psi]\!]^m = [\![\varphi]\!]^m \cap [\![\psi]\!]^m (= \cap \circ \langle [\![\varphi]\!]^m, [\![\psi]\!]^m\rangle), \qquad (3)$$

$$[\![\varphi \vee \psi]\!]^m = [\![\varphi]\!]^m \cup [\![\psi]\!]^m.$$

Розглянемо квантори підмножин. Припустимо, що φ має вільно тільки змінні v_1, v_2, v_3 і (при умові, що *m* = 3) функція $[\![\varphi]\!]^3 : A^3 \to 2$ вже визначена. Необхідно визначити функцію $[\![\forall v_3 \varphi]\!]^3 : A^3 \to 2$. Візьмемо вільну трійку $\langle x_1, x_2, x_3\rangle \in A^3$ і положимо визначення виконаності:

$$B_2 = \{x \in A : \mu \vDash \varphi[\overline{x_1, x_3}]\} = .\{x \in A : [\![\varphi]\!]^3(\overline{x_1, x_3}) = 1\}.$$

З цього визначення слідує, що $\mu \vDash \forall v_3 \varphi[\overline{x_1, x_3}]$ тоді і тільки тоді, коли $B_2 = A$. Тому покладемо:

$$[\![\forall v_3 \varphi]\!]^3(\langle\overline{x_1, x_3}\rangle) = \begin{cases} 1, \text{якщо } B_2 = A, \\ 0 \text{ в іншому випадку.} \end{cases}$$

Співпідставлення трійці $\overline{x_1, x_3}$ підмножини $B_2 \subseteq A$ визначає функцію $|\varphi|_2^3$ з A^3 у $\mathcal{P}(A)$. Введемо нову функцію $\forall_A : \mathcal{P}(A) \to 2$, маючи:

$$\forall_A(B) = \begin{cases} 1, \text{якщо } B = A, \\ 0, \text{якщо } B \neq A. \end{cases}$$

Тоді функцію $[\![\forall v_3 \varphi]\!]^3$ можна записати у вигляді $[\![\forall v_3 \varphi]\!]^3 = \forall_A \circ |\varphi|_2^3$. Ця функція має вигляд, представлений на рис. 1.

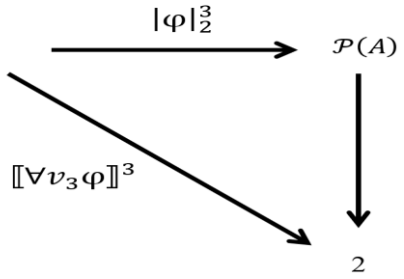

Рис. 1. Граф комутативної діаграми функції $[\![\forall v_3 \varphi]\!]^3$

Необхідно дати категорне визначення для $\forall_A$. Таке визначення дано в [2], де $\forall_A$ визначається як характеристичне відображення імені функції $true_A$. Тобто визначається $[true_A]: 1 \to 2^A$– ім'я функції $true_A$ – як стрілку (функцію), яка виділяє $true_A$ з множини 2^A. Так як $true_A = \chi_A: A \to 2$, отождествляємо $true_A$ з $\{A\} \subseteq \mathcal{P}(A)$. Характеристичною функцією цього підоб'єкту є $\forall_A$. Функція $[true_A]$ сама є експоненціально приєднаною до композиції, яка наданана рис. 2.

$$1 \times A \xrightarrow{pr_A} A \xrightarrow{true_A} 2$$

Рис. 2. Категорне проектне визначення відображення $|\psi|_2^4$

де $pr_A(\langle 0, x\rangle) = x$. Таким чином, у рівнянні $[\![\forall v_2 \varphi]\!]^3 = \forall_A \circ |\varphi|_2^3$ через $\forall_A$ визначена характеристична функція підоб'єкту у 2^A, яка визначається вкладенням, експоненціально приєднаним до $true_A \circ pr_A$, а $|\varphi|_2^3$ визначає функцію, експоненціально приєднаною до $[\![\varphi]\!]^3 \circ \langle pr_1^4, pr_4^4, pr_3^4\rangle$.

Для квантора існування аналогічним образом розраховуємо:

$\mu \vDash \exists v_2 \varphi[\overline{x_1, x_3}]$ тоді і тільки тоді $B_2 \neq 0$. (4)

Тому покладемо:

$$[\![\exists v_2 \varphi]\!]^3(\langle \overline{x_1, x_2}\rangle) = \begin{cases} 1, \text{ якщо } B_2 \neq 0, \\ 0 \text{ у іншому випадку.} \end{cases} \quad (5)$$

З (5) витікає, що діаграма графа, наведеного на рис. 3 є комутативною, де:

$$\exists_A(B) = \begin{cases} 1, \text{якщо } B \neq \varnothing, \\ 0, \text{якщо } B = \varnothing. \end{cases} \quad (6)$$

Функція $\exists_A$ є характеристичною для множини:

$$C = \{B: B \neq \varnothing\} = \{B: \text{існує } x, \text{який належить } A, \text{такий, що } x \in B\}.$$

Якщо $\in_A \hookrightarrow \mathcal{P}(A) \times A$ – відношення належності на А, тобто:

$$\in_A = \{\langle B, x\rangle: B \subseteq A \text{ і } x \in B\},$$

і p_A– перша проекція добутку,

$\mathcal{P}(A) \times A$ у $\mathcal{P}(A)$: $(p_A(\langle B, x\rangle) = B)$, то $p_A(\in_A) = C$.

Таким чином, $\exists_A$ є характеристичною функцією образу композиції:

$$\in_A \hookrightarrow \mathcal{P}(A) \times A \xrightarrow{p_A} \mathcal{P}(A). \quad (7)$$

Загальне визначення функцій $[\![\forall v_i \varphi]\!]^m$ і $[\![\exists v_i \varphi]\!]^m$ отримуємо з приведеного підстановкою *m* замість 4 і *i* замість 2.

Функцію $[\![t \approx u]\!]^m: A^m \to 2$ визначимо так:

$$[\![t \approx u]\!]^m(\langle \overline{x_1, x_m} \rangle) = \begin{cases} 1, \text{якщо } x_t = x_u, \\ 0 \text{ у іншому випадку,} \end{cases}$$

де *x* – деяка (вільна) оцінка, перші *m* членів якої співпадають з $\overline{x_1, x_m}$. Таким чином, отримуємо комутативну діаграму графу, яка надана на рис. 5.

$p_t^m: A^m \to A, p_u^m: A^m \to A$ і δ_A визначені співвідношеннями:

$$p_t^m(\langle \overline{x_1, x_m} \rangle) = x_t, \quad p_u^m(\langle \overline{x_1, x_m} \rangle) = x_u,$$
$$\delta_A(\langle x, y \rangle) = \begin{cases} 1, \text{якщо } x = y, \\ 0, \text{якщо } x \neq y, \end{cases} x, y \in A.$$

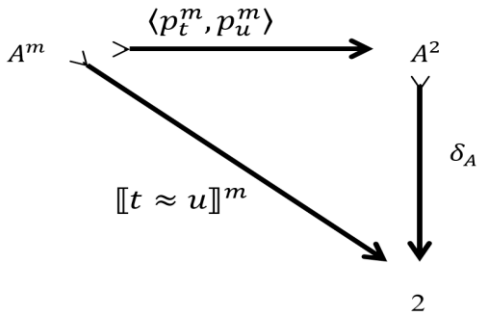

Рис. 5. Граф комутативної діаграми функції $[\![t \approx u]\!]^m$

Функція δ_A є характеристичною функцією тотожного відношення (діагоналі) $\Delta = \{\langle x, y \rangle: x = y\} \subseteq A^2$. Функція може бути ототожнена з монострілкою $1_A: A \to A^2$, яка переводе *x* у $\langle x, x \rangle$. Для категорного визначення p_t^m введемо функцію $f_c: \{0\} \to A$, покладемо $f_c(0) = c$. Тоді:

$$p_t^m = \begin{cases} pr_i^m: A^m \to A, \text{якщо } t = v_i, \\ f_c \circ !: A^m \xrightarrow{1} 1 \xrightarrow{f_c} A, \text{якщо e} = \text{c} \end{cases}$$

Подібні рівняння справедливі і для p_u^m.

Переходячи до предикатної форми, визначимо через $r: A^2 \to 2$ характеристичну функцію множини $R \subseteq A \times A$. Тоді діаграма, яка представлена на рис. 6, буде комутативною.

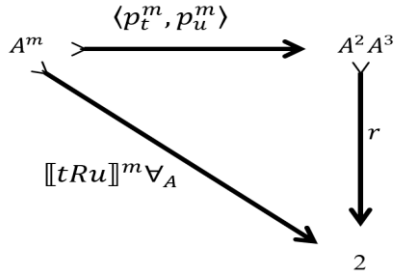

Рис. 6. Граф комутативної діаграми функції $[\![tRu]\!]^m$

Наскільки істинна модель і як це можна описати. Нехай формула $\varphi(\overline{v_{i_1}, v_{i_n}})$ має індекс *n*, тоді визначаючи $[\![\varphi]\!]\mu: A^n \to 2$ умовами:

$$[\![\varphi]\!]\mu(\langle \overline{x_1, x_n} \rangle) = \begin{cases} 1, \text{якщо } \mu \vDash \varphi[\overline{x_1, x_n}], \\ 0 \text{ у іншому випадку,} \end{cases}$$

отримуємо: $\mu \vDash \varphi$ тоді і тільки тоді, коли для будь-яких $\overline{x_1, x_n} \in A$ має місце:

$$[\varphi]_\mu(\langle \overline{x_1, x_n} \rangle) = 1 \Longrightarrow [\varphi]\mu = \chi_{A^n} \Longrightarrow [\varphi]\mu = true A^n.$$

Для опису функції $[\varphi]_\mu$ у вигляді графу визначимо, що існує m – необхідне для φ число, таке, що $\mu \vDash \varphi[\overline{x_1, x_n}]$ тоді і тільки тоді, коли для будь-яких $\overline{y_1, y_m}$, має місце $\mu \vDash \varphi[\overline{y_1, y_m}]$. Таким чином, для будь-якого *f*, яке задовольняє рівнянню $pr_{i_k}^m \circ f = pr_k^n$ при $1 \leq k \leq n$ граф діаграми, який наведений на рис. 7. буде комутативний.

Цій опис функції $[\varphi]\mu$ придатний для визначення істинності пропозицій, які виникають під час аналізу істинності проектування впливу загроз на механізми захисту інформації.

Вільний елемент множини A^n, тобто *n*-членну послідовність, можна розглядати як функцію з ординалу $n = \{0,1, \dots, n-1\}$ у A. Тому, якщо $n = 0,$ то A^0 є множиною функцій з ординалу 0 (початкового об'єкту ∅) у *A*. Таким чином, $A^0 = A^\emptyset = \{\emptyset\} = 1$.

Якщо індекс φ=0, то $[\![\varphi]\!]_\mu : A^0 \to 2$ є деяким істинним значенням $1 \to 2$; при цьому:

$$[\varphi]_\mu = \begin{cases} true, \text{якщо } \mu \vDash \varphi, \\ false \text{ у іншому випадку.} \end{cases} \quad (8)$$

На основі (8) можна зробити наступний висновок, що для будь-якого $m \geq 1$ і будь-якого $f: 1 \to A^m$ граф діаграми, який наведений на рис. 8 є комутативним, і при $\mu \vDash \varphi$, функція $[\![\varphi]\!]^m$ приймає значення 1, якщо не виконуються вимоги, то ця функція приймає значення 0.

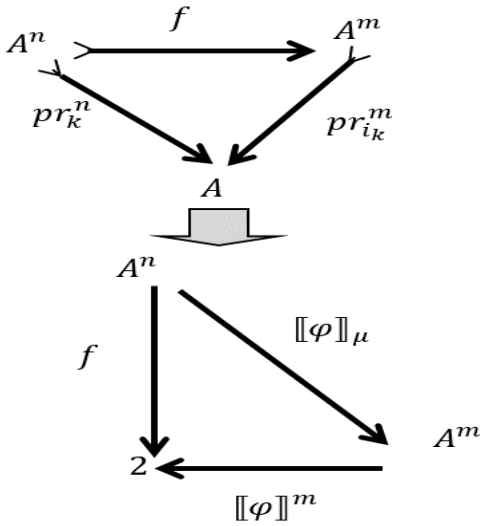

Рис. 7. Граф комутативної діаграми істинності функції $[\![\varphi]\!]_\mu$

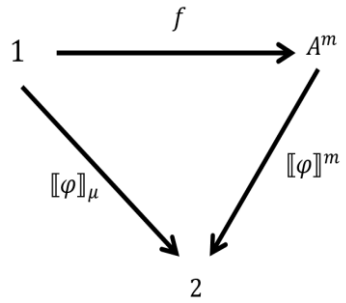

Рис. 8. Загальний граф комутативної діаграми функції $[\varphi]_\mu$ для будь-якого $m \geq 1$ і будь-якого $f: 1 \to A^m$

Звертаючись до моделі системи захисту інформації з повним перекриттям загроз [3] розкриємо порядок впливу загроз на механізми захисту. Для чого визначимо взаємозв'язки між елементами області загроз, механізмами захисту, системою аналізу загроз та областю захисту, як надано на рис. 9, де $t_1, t_2, \dots, t_i$ – загрози з області загроз, $u_1, u_2, \dots, u_d$ – підмножин уразливостей механізмів захисту, $b_1, b_2, \dots, b_d$ – підмножин бар'єрів захисту (фільтрів) ($\overline{1,k}$ – порядковий номер класу механізмів захисту), $h_1, h_2, \dots, h_y$ – підмножин системи аналізу загроз,$v_1, v_2, \dots, v_j$ – множини областей захисту інформаційної системи.

Усі підмножини знаходяться у тісних взаємозв'язках між собою.

Якщо об'єднати окремі підмножини у множини (рис. 9), тоді можна побудувати комутативний граф взаємовідносин множин загроз та підмножин множини системи захисту інформації, який представлений на рис. 10.

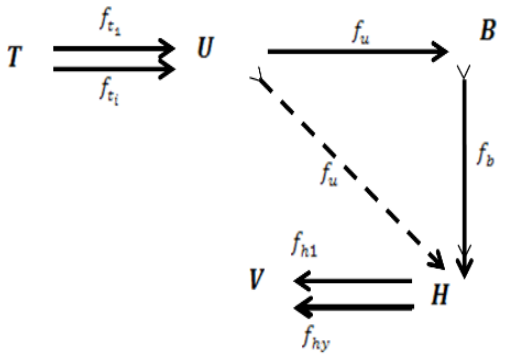

Рис. 10. Комутативний граф взаємовідносин множин загроз та підмножин множини системи захисту інформації

З рисунка 10 можна зробити висновок, що згідно [1] коприрівнювачем пари паралельних β-стрілок f_{t_1}, f_{t_i} є комежа $f_{t_1}, f_{t_i}: \boldsymbol{T} \rightrightarrows \boldsymbol{U}$. Коприрівнювач можна розглядати як таку β-стрілку $f_u: u \to h$ при якій: $f_u \circ f_{t_1} = f_u \circ f_{t_i}$ та будь-яку стрілку $f_u: u \to h$, яка задовольняє рівнянню $f_u \circ f_{t_1} = f_u \circ f_{t_i}$ існує одна єдина стрілка $f_b: b \to h$, для якої діаграма комутативна.

У подальшому, при розгляді місця множини ***H*** у системі захисту інформації згідно [2], можна побудувати наступний граф, який представлений на рис. 11.

Якщо $f_b \subseteq f_h$ і $f_h \subseteq f_b$, то f_b і f_h пропускаються друг через друга, і

$$f_b = f_h \circ f_{b^*}, \qquad f_h = f_b \circ f_{h^*}.$$

У цілому, якщо множина ***M*** (механізмів захисту) є підмножиною множини ***A*** (процесу захисту інформації), то функція включення $M \hookrightarrow \mathrm{A}$ іньєктивна і тому мономорфна. З іншого боку, вільна мономорфна функція $f: U \rightarrowtail B$ визначає підмножину множини ***B***, при якій $\mathrm{Im} f = \{f(x): x \in U\}$Тобто, f індуцирує бієкцію між *U* та *Im f*, далі отримуємо $U \cong \mathrm{Im}\, f$.

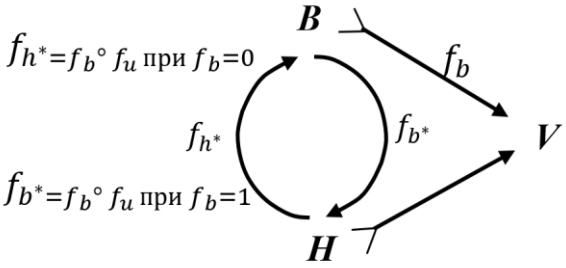

Рис. 11. Діаграма тождественості підмножин при: $f_b = f_h \circ f_{b^*}$, $f_h = f_b \circ f_{h^*}$

Крім того, підмножини системи захисту інформації знаходяться, між собою, у взаємозв'язках, які можна описати наступним чином:

$$\boldsymbol{U} = \begin{array}{l} pr\ t_s^i\left(\langle u_1^1, u_1^2, \dots, u_1^k\rangle\right) = u_1^k; \\ pr\ b_1^w\left(\langle u_2^1, u_2^2, \dots, u_2^k\rangle\right) = u_2^k; \\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots \\ pr\ b_2^w\left(\langle u_d^1, u_d^2, \dots, u_d^k\rangle\right) = u_d^k. \end{array}$$

$$\boldsymbol{B} = \begin{matrix} pr\ u_1^k(\langle b_1^1, b_1^2, \dots, b_1^w\rangle) = b_1^w; \\ pr\ u_2^k(\langle b_2^1, b_2^2, \dots, b_2^w\rangle) = b_2^w; \\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots \\ pr\ u_d^k\big(\langle b_d^1, b_d^2, \dots, b_d^k\rangle\big) = b_d^w. \end{matrix}$$

$$\boldsymbol{H} = \begin{matrix} u_1^k b_1^w \\ u_2^k b_2^w \\ \dots\ \dots \\ u_d^k b_d^w \end{matrix}$$

Таким чином, область визначення мономорфної функції *B* ізоморфна деякій підмножині області значень цієї функції *U*. Іншою мовою, область визначення–підмножина *u* є, з точністю до ізоморфізма, підмножиною області значень-множини *b*, тобто $f: u \rightarrowtail b$.

У загальному випадку представимо процес захисту інформації який наданий на рис. 9, 10. 11, отримуємо декартовий квадрат, який наданий на рис. 12.

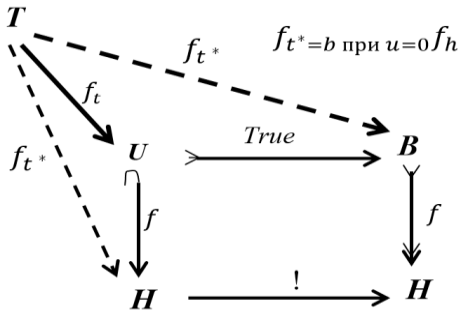

Рис. 12. Комутативна діаграма декартового квадрату

Дійсно, якщо уявити що зовнішній “квадрат”, як комутативний, тоді, якщо $t \in T$ і $f\big(f(t)\big) = \text{true}\big(!(H)\big) = U$, то $f(b) \in H$, $f(u) \in H$. Тому при $f_t^*: T \to H, B$, яке визначено рівнянням $f_t(T) = f_{t^*}(T)$, уся діаграма буде комутативною, але при одному f_t. Відповідно, якщо $U \subseteq B$, то квадрат, представлений на рис. 12. декартовий.

Відношення еквівалентності на множині $\boldsymbol{H}$ по визначенню – відношення $R \subseteq \boldsymbol{H} \times A$ 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:$[a] = \{b: aRb\}$, 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 класи еквівалентності не мають загальних елементів.
- $a \in [a]$. Тобто кожна $a \in A$ є елементом одного і того-ж класу *R*-еквівалент-ності.
-

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

$$A/_R = \{[a]: a \in A\}. \qquad (9)$$

Цей перехід виконується за допомогою природного відображення:

$$f_R: A \to {}^{A}/_{R}, \text{ де } f_R(a) = [a], \text{для } a \in A.$$

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:

$$f(\langle a, b\rangle) = a \text{ і } g(\langle a, b\rangle) = b. \qquad (10)$$

Висновок

Математична модель проектних відносин загроз та множин системи захисту інформації дозволяє на рівні математичних множин прогнозувати порядок побудови тих, або інших множин або підмножин систем захисту інформації, проводити аналіз правильності побудови цих множин. Запропонований математичний апарат дозволяє більш практично визначати загальний порядок побудови структури систем захисту інформації на етапі ескізного проектування. Це є вхідними даними для системи автоматичного проектування побудови систем захисту інформаці

Література

1. Аналіз систем та методів виявлення несанкціонованих вторгнень у комп'ютерні мережі [Електронний ресурс] / В. В. Литвинов [та ін.] // Математичні машини і системи. К : ІПММС НАН України, 2018. № 1. С. 31-40.
2. Сучасні методи виявлення аномалій в системах виявлення вторгнень / О.М. Колодчак // Вісник Національного ун-т «Львівська політехніка». Комп'ютерні системи та мережі. 2012. № 745. С. 98-104.
3. Дослідження методів виявлення вторгнень в телекомунікаційні системи та мережі / Д. О. Даниленко, О. А. Смірнов, Є. В. Мелешко // Системи озброєння і військова техніка. Х. : Харк. нац. ун-т Повітряних Сил ім. І. Кожедуба, 2012. № 1. С. 92-100.
4. The State of the Art in Intrusion Prevention and Detection [Electronic resourse] / Al-Sakib Khan Pathan. New York : Auerbach Publications, 2014.
5. Analysis of Host-Based and Network-Based Intrusion Detection System / Amrit Pal Singh, Manik Deep Singh. India : I. J. Computer Network and Information Security, 2014. Vol. 8. 41-47 pp.
6. Аналіз сучасних систем виявлення атак і запобігання вторгненням / А. А.Завада, О. В. Самчишин, В. В. Охрімчук // Інформаційні системи. Житомир : Збірник наукових праць ЖВІ НАУ, 2012. Т. 6, № 12. С. 97-106.
7. An implementation of intrusion detection system using genetic algorithm / Mohammad Sazzadul Hoque, Md. Abdul Mukit, Md., Abu Naser Bikas // International Journal of Network Security & Its Applications (IJNSA). Sylhet, 2012. Vol. 4, No. 2. P. 109-120.
8. Analysis and Evaluation of Network-Based Intrusion Detectionand Prevention System in an Enterprise Network Using Snort Freeware / O. B. Lawal [et al.] // African Journal of Computing & ICT. Ibadan, 2013. Vol. 6, No. 2. P. 169-184.
9. IDS / IPS. Netgate Documentation: [website]. Washington : Rubicon Communications LLC, 2017. [Electronic resource]. Online: https://www.netgate. com/docs/pfsense/ids-ips/.
10. Довбешко С.В., Толюпа С.В., Шестак Я.В. Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак. Науково-технічний журнал "Сучасний захист інформації".– №1. 2019. С. 56-62.
11. Toliupa S., Nakonechnyi V., Uspenskyi O. Signature and statistical analyzers in the cyber attack detection system. Information technology and security. Ukrainian research papers collection Volume 7, Issue 1 (12). c. 69-79.
12. Толюпа С.В., Штаненко С.С., Берестовенко Г. Класифікаційні ознаки систем виявлення атак та напрямки їх побудови. Збірник наукових праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут Випуск № 3. 2018р. с. 56-66.
13. Toliupa S.1, Druzhynin V.2, Parkhomenko I Signature and statistical analyzers in the cyber attack detection system. Scientific and Practical Cyber Security Journal (SPCSJ) № 3 (02) pp. 47-53.
14. Павлов І.М. Функторність та гранічність відображень об'єктів множин в системах захисту інформації / І.М. Павлов, В.О. Хорошко. – "Інформаційна безпека". – К.: 2013. – № 1(9). – С. 107 – 116
15. Павлов І.М. Альмагами, повнота діаграм та підоб'єкти множин в системах захисту інформації / І.М. Павлов. – Інформатика та математичні методи в моделюванні. – ОНПІ.: 2013. – Т.3. – № 1. – С. 50 – 60.

References

1. Analysis of systems and methods for detecting unauthorized intrusions into computer networks [Electronic resource] / VV Litvinov [etc.] // Mathematical Machines and Systems. K: IPMMS NAS of Ukraine, 2018. № 1. P. 31-40.
2. Modern methods of detecting anomalies in intrusion detection systems / O.M. Kolodchak // Bulletin of the National University "Lviv Polytechnic". Computer systems and networks. 2012. № 745. pp. 98–104.
3. Research of methods of detection of intrusions into telecommunication systems and networks / DO Danilenko, OA Smirnov, EV Meleshko // Weapons systems and military equipment. H .: Hark. nat. University of the Air Force. I. Kozheduba, 2012. № 1. S. 92-100.

4. The State of the Art in Intrusion Prevention and Detection [Electronic resourse] / Al-Sakib Khan Pathan. New York: Auerbach Publications, 2014.

5. Analysis of Host-Based and Network-Based Intrusion Detection System / Amrit Pal Singh, Manik Deep Singh. India: I. J. Computer Network and Information Security, 2014. Vol. 8. 41-47 pp.

6. Analysis of modern systems for detecting attacks and preventing intrusions / AA Zavada, OV Samchyshyn, VV Okhrimchuk // Information systems. Zhytomyr: Collection of scientific works of ZhVI NAU, 2012. Vol. 6, № 12. P. 97-106.

7. An implementation of intrusion detection system using genetic algorithm / Mohammad Sazzadul Hoque, Md. Abdul Mukit, Md., Abu Naser Bikas // International Journal of Network Security & Its Applications (IJNSA). Sylhet, 2012. Vol. 4, no. 2. P. 109-120.

8. Analysis and Evaluation of Network-Based Intrusion Detectionand Prevention System in an Enterprise Network Using Snort Freeware / O. B. Lawal [et al.] // African Journal of Computing & ICT. Ibadan, 2013. Vol. 6, no. 2. P. 169-184.

9. IDS / IPS. Netgate Documentation: [website]. Washington: Rubicon Communications LLC, 2017. [Electronic resource]. Online: https: //www.netgate. com / docs / pfsense / ids-ips /.

10. Dovbeshko SV, Tolyupa SV, Shestak Ya.V. Application of data mining methods to build attack detection systems. Scientific and technical journal "Modern information protection". - “1. 2019. S. 56-62.

11. Toliupa S., Nakonechnyi V., Uspenskyi O. Signature and statistical analyzers in the cyber attack detection system. Information technology and security. Ukrainian research papers collection Volume 7, Issue 1 (12). with. 69-79.

12. Toliupa SV, Shtanenko SS, Berestovenko G. Classification features of attack detection systems and directions of their construction. Collection of scientific works of the Military Institute of Telecommunications and Informatization named after the Heroes of Kruty Issue № 3. 2018. with. 56-66.

13. Toliupa S.1, Druzhynin V.2, Parkhomenko I Signature and statistical analyzers in the cyber attack detection system. Scientific and Practical Cyber Security Journal (SPCSJ) № 3 (02) pp. 47-53.

14. Pavlov IM Functionality and boundary of mappings of sets of objects in information protection systems / I.M. Павлов, B.O. Good. ¬– “Information Security”. - K .: 2013. - № 1 (9). - P. 107 - 116

15. Pavlov IM Almags, completeness of diagrams and subsets of sets in information protection systems / I.M. Pa-catch. - Informatics and mathematical methods in modeling. - ONPI .: 2013. - Vol.3. - № 1. - P. 50 - 60.