УДК 004.415.056.5(075)
DOI 10.17721/ISTS.2023.1.28-36

Сергій Толюпа, orcid.org/0000-0002-1919-9174,
tolupa@i.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна,
Сергій Штаненко, orcid.org/0000-0001-9776-4653,
shsergei@ukr.net
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна

МАТЕМАТИЧНА МОДЕЛЬ ВЗАЄМОВІДНОСИН СИСТЕМИ КЕРУВАННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Результативне розв'язання задач аналізу і синтезу систем керування інформаційною безпекою не можна забезпечити одними лише способами простого опису їхньої поведінки в різних умовах – системотехніка виявила проблеми, які потребують кількісного оцінювання характеристик. Ті дані, що отримані експериментально або шляхом математичного моделювання, повинні розкривати властивості систем керування інформаційною безпекою. Основним у них є ефективність, під якою розуміють ступінь відповідності результатів захисту інформації поставленій меті. Остання, залежно від наявних ресурсів, знань розробників та інших факторів, може бути досягнута тією або іншою мірою, причому можливі альтернативні шляхи її реалізації. У ряді публікацій авторами запропоновано основи категорійного апарату теорії множин, які дозволяють пояснити процес взаємовідносин множин загроз і множин системи захисту інформації, що дозволяє будувати різні математичні моделі з метою аналізу систем інформаційного обміну в системах критичного застосування. Нині створення систем керування інформаційною безпекою неможливе без дослідження й узагальнення світового досвіду побудови інформаційних систем та їхніх складових підсистем, одними з ключових серед 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 має забезпечити адекватність моделювання процесів захисту інформації за будь-яких умов впливу кіберзагроз. Під час визначення 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 мають контролювати правильність роботи процесу захисту інформації. У статті проаналізовано різні варіанти побудови моделей системи керування інформаційною безпекою та створено математичну модель, яка враховує внутрішні взаємозв'язки різних підмножин складових системи захисту інформації за впливу кіберзагроз.

Ключові слова: *граф, діаграми, кіберзагрози, множини, моделі, функції, підмножини, проєктування, система захисту інформації, керування інформаційною безпекою.*

1. ВСТУП

Процес розвитку й упровадження новітніх інформаційних технологій забезпечує безпрецедентні умови для накопичення і використання інформації, а також створює фундаментальну залежність від їхнього нормального функціонування всіх сфер життєдіяльності суспільства та держави: економіки, політики, сфери національної та міжнародної безпеки тощо. Така залежність стає вразливим місцем у функціонуванні систем та 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 й інформаційним системам. Експерти передбачають, що в прийдешньому році повністю зміниться структура кібероперацій і методи їхнього проведення.

Масовані кібератаки ініціюють створення спеціальних технічних рішень, засобів і систем

протидії. Для виявлення мережних вторгнень використовують сучасні методи [1–3], моделі [4, 5], засоби [6–9] і комплексні технічні рішення для систем виявлення та запобігання вторгнень [9–12], які можуть залишатись ефективними у разі появи нових або модифікованих видів кіберзагроз. Проте на практиці під час появи нових загроз та аномалій, породжених атакуючими діями з невстановленими або нечітко визначеними властивостями, зазначені засоби не завжди є ефективними і вимагають тривалих часових ресурсів для їхньої відповідної адаптації.

Сьогодні вирішення питань забезпечення безпеки в інформаційних системах (ІС) та керування станом їхньої захищеності описують роботи вітчизняних і зарубіжних дослідників: В. Л. Бурячок, С. О. Гнатюк, О. Г. Корченко, О. О. Кузнецова, І. Ю. Субача, В. О. Хорошко, С. П. Євсеєва, В. Б. Дудикевич, Л. Т. Пархуця, T. Ptaceka, G. Elmasry, P. Albers, O. Camp та ін.

Нині створення систем керування інформаційною безпекою неможливе без дослідження й узагальнення світового досвіду побудови інформаційних систем та їхніх 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 має забезпечити адекватність моделювання процесів захисту інформації для будь-яких умов впливу кіберзагроз.

2. ПОСТАНОВКА ПРОБЛЕМИ

У 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 запропоновано математичний апарат теорії топосів, який дозволяє на рівні спеціальних категорій будувати моделі для теоретико-множинних конструкцій етапу ескізного проєктування систем захисту інформації [13, 14].

3. ОСНОВНА ЧАСТИНА

Моделлю для множин процесу захисту інформації з повним перекриттям загроз є структура $\mu = \langle A, R, c\rangle$, яка складається з непорожньої 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 c – конкретного індивіду підмножин R, зазначимо, що $c \in A$.

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

Згідно з інтерпретацією змінних 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 – значення змінної v_i, яке 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 $y_i = x_i$ у будь-якому разі, коли v_i входить вільно у φ. Ця модель $\mu = \langle A, R, c\rangle$, вимога φ^m (належне φ число m – кратного добутку), тобто $\varphi^m = \{\langle \overline{x_1, x_m}\rangle : \mu = \varphi[\overline{x_1, x_m}]\}$ являє собою множину всіх 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. Причому 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, перетин множин φ^m іншого перетину множин ψ^m складається з послідовностей, які задовольняють вимогу $\varphi \wedge \psi$. Отже, отримуємо

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

Тобто, якщо m є необхідним для φ і ψ числом, то воно буде необхідним і для $\varphi \wedge \psi$.

Розглянемо підоб'єкти і їхні характеристичні стрілки.

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

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

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

$$[\![\sim\varphi]\!]^m = \neg \circ [\![\varphi]\!]^m,$$
$$[\![\varphi \wedge \psi]\!]^m = [\![\varphi]\!]^m \cap [\![\psi]\!]^m (= \cap \circ \langle [\![\varphi]\!]^m, [\![\psi]\!]^m\rangle),$$
$$[\![\varphi \vee \psi]\!]^m = [\![\varphi]\!]^m \cup [\![\psi]\!]^m. \quad (3)$$

Розглянемо квантори підмножин. Припустимо, що φ має вільні тільки змінні v_1, v_2, v_3 і (за умови, 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 припустимо визначення виконуваності:

$$B_2 = \{x \in A: \mu \vDash \varphi[\overline{x_1, x_3}]\} =.$$

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

Із 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

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

Зіставлення $\overline{x_1, x_3}$ підмножини $B_2 \subseteq A$ визначає функцію $|\varphi|_2^3$ з A^3 у $\mathcal{P}(A)$. Уведемо 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, зображений на рис. 1.

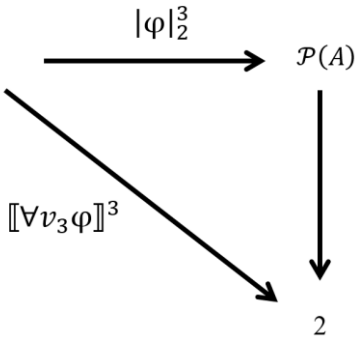

Рис. 1. Граф комутативної діаграми функції $[\![\forall v_3 \varphi]\!]^3$

Необхідно дати категорійне визначення для $\forall_A$. Таке визначення дано в [2], де $\forall_A$ визначається як характеристичне відображення імені функції $true_A$. Тобто визначається $\lceil true_A \rceil: 1 \to 2^A$– ім'я функції $true_A$ – як стрілку (функцію), яка виділяє $true_A$ з множини 2^A. Оскільки $true_A = \chi_A: A \to 2$, ототожнюємо $true_A$ з $\{A\} \subseteq \mathcal{P}(A)$. Характеристичною функцією цього підоб'єкта є $\forall_A$. Функція $\lceil true_A \rceil$ сама є експоненціально приєднаною до композиції, зображеної на рис. 2, де $pr_A(\langle 0, x\rangle) = x$.

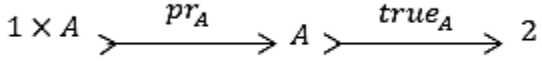

Рис. 2. Категорійне проєктне визначення відображення $|\psi|_2^4$

Таким чином, у рівнянні $[\![\forall v_2 \varphi]\!]^3 = \forall_A \circ |\varphi|_2^3$ через $\forall_A$ визначена характеристична функція підоб'єкта 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

$$\mu \vDash \exists v_2 \varphi[\overline{x_1, x_3}] \text{ тоді і тільки тоді,}$$

$$\text{якщо } B_2 \neq 0. \quad (4)$$

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) випливає, що діаграма графа з 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

$$C = \{B: B \neq \varnothing\} =$$

$$= \begin{Bmatrix} B: \text{існує } x, \text{який належить } A, \\ \text{такий, що } x \in B \end{Bmatrix}.$$

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

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

і p_A – перша проєкція добутку,

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

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 підстановкою m замість (4) та i замість (2).

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

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

де x – деяка (вільна) оцінка, перші m членів якої збігаються з $\overline{x_1, x_m}$. Таким чином, отримуємо комутативну діаграму графа (рис. 3).

На рис. 3 $p_t^m: A^m \to A, p_u^m: A^m \to A$ і δ_A визначені співвідношеннями:

$$p_t^m(\langle\overline{x_1, x_m}\rangle) = x_t, \quad p_u^m(\langle\overline{x_1, x_m}\rangle) = x_u,$$

$$\delta_A(\langle x, y\rangle) = \begin{cases} 1, \text{якщо } x = y, \\ 0, \text{якщо } x \neq y, \end{cases} x, y \in A.$$

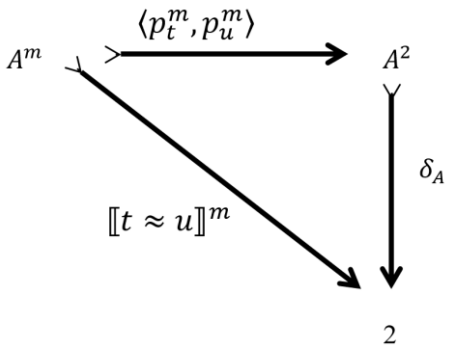

Рис. 3. Граф комутативної діаграми функції $[\![t \approx u]\!]^m$

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 переводить x у $\langle x, x\rangle$. Для категорійного визначення p_t^m уведемо функцію $f_c : \{0\} \to A$, покладемо $f_c(0) = c$. Тоді

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

Подібні рівняння справедливі і для p_u^m.

Перейшовши до предикатної форми, визначимо через $r : A^2 \to 2$ характеристичну функцію множини $R \subseteq A \times A$. Тоді діаграма на рис. 4 буде комутативною.

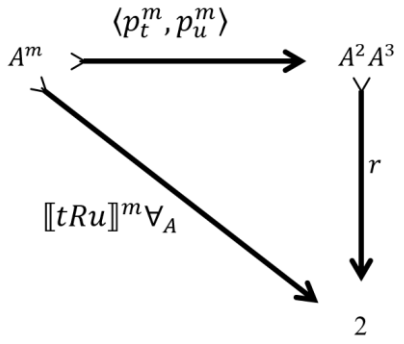

Рис. 4. Граф комутативної діаграми функції $[\![tRu]\!]^m$

Розглянемо 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 графа 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 $\overline{y_1, y_m}$ справедливе $\mu \vDash \varphi[\overline{y_1, y_m}]$. Таким чином, для будь-якого f, яке задовольняє рівняння $pr_{i_k}^m \circ f = pr_k^n$ при $1 \le k \le n$, граф діаграми, зображений на рис. 7, буде комутативний.

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

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

$$A^0 = A^{\varnothing} = \{\varnothing\} = 1.$$

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

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

На основі (8) можна дійти висновку, що для будь-якого $m \ge 1$ і будь-якого $f : 1 \to A^m$ граф діаграми, зображений на рис. 5, є комутативним, і при $\mu \vDash \varphi$ функція $[\![\varphi]\!]^m$ набуває значення 1, якщо не виконуються вимоги, то ця функція набуває значення 0.

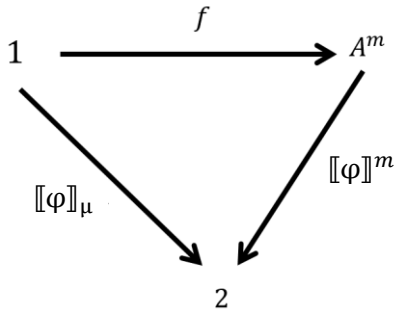

Рис. 5. Загальний граф комутативної діаграми функції $[\varphi]_\mu$ для будь-якого $m \ge 1$ і будь-якого $f : 1 \to A^m$

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 показано на рис. 6, де $t_1, t_2, \dots, t_i$ – загрози з області загроз, $u_1, u_2, \dots, u_d$ – підмножини уразливостей механізмів захисту, $b_1, b_2, \dots, b_d$ – підмножини 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 тісно взаємно пов'язані між собою.

Якщо об'єднати окремі підмножини у множини (рис. 6), то можна побудувати комутативний граф взаємовідносин множин загроз і підмножин множини системи захисту інформації, який показано на рис. 6.

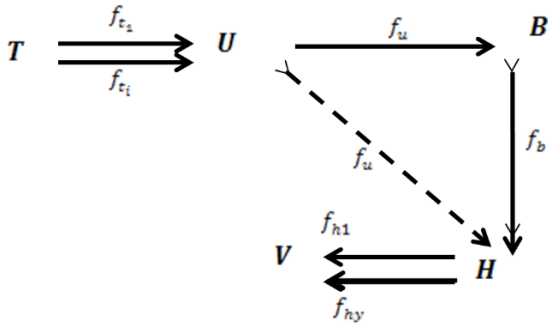

Рис. 6. Комутативний граф взаємовідносин множин загроз і підмножин множини системи захисту інформації

З рис. 7 можна дійти висновку, що згідно з [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 рівняння $f_u \circ f_{t_1} = f_u \circ f_{t_i}$, існує одна єдина стрілка $f_b: b \to h$, для якої діаграма комутативна.

У подальшому, розглядаючи місця множини $\boldsymbol{H}$ у системі захисту інформації, згідно з [2], можна побудувати наступний граф, який зображено на рис. 7.

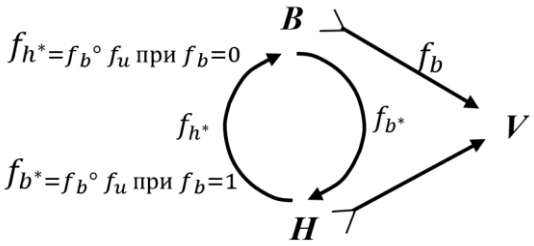

Рис. 7. Діаграма тотожності підмножин при $\boldsymbol{f_b = f_h \circ f_{b^*}}$, $\boldsymbol{f_h = f_b \circ f_{h^*}}$

Якщо $f_b \subseteq f_h$ і$f_h \subseteq f_b$, то f_b і f_h пропускаються один через одного, і $f_b = f_h \circ f_{b^*}$, $f_h = f_b \circ f_{h^*}$.

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

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

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

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

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

Таким чином, область визначення мономорфної функції $\boldsymbol{B}$ ізоморфна деякій підмножині області значень цієї функції $\boldsymbol{U}$. 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, зображений на рис. 6, 7, 8, отримуємо декартовий квадрат, який показано на рис. 9.

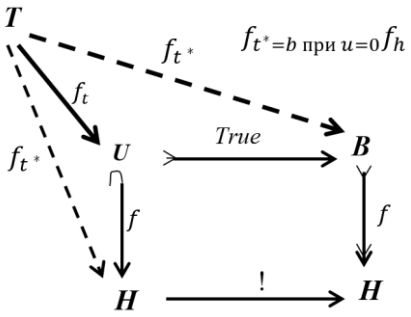

Рис. 9. Комутативна діаграма декартового квадрата

Дійсно, якщо уявити зовнішній "квадрат", як комутативний, тоді, якщо

$$t \in T \text{ і } f\left(f(t)\right) = \mathrm{true}\left(!\,(H)\right) = U,$$
$$\text{то } f(b) \in H, f(u) \in H.$$

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, зображений на рис. 12, декартовий.

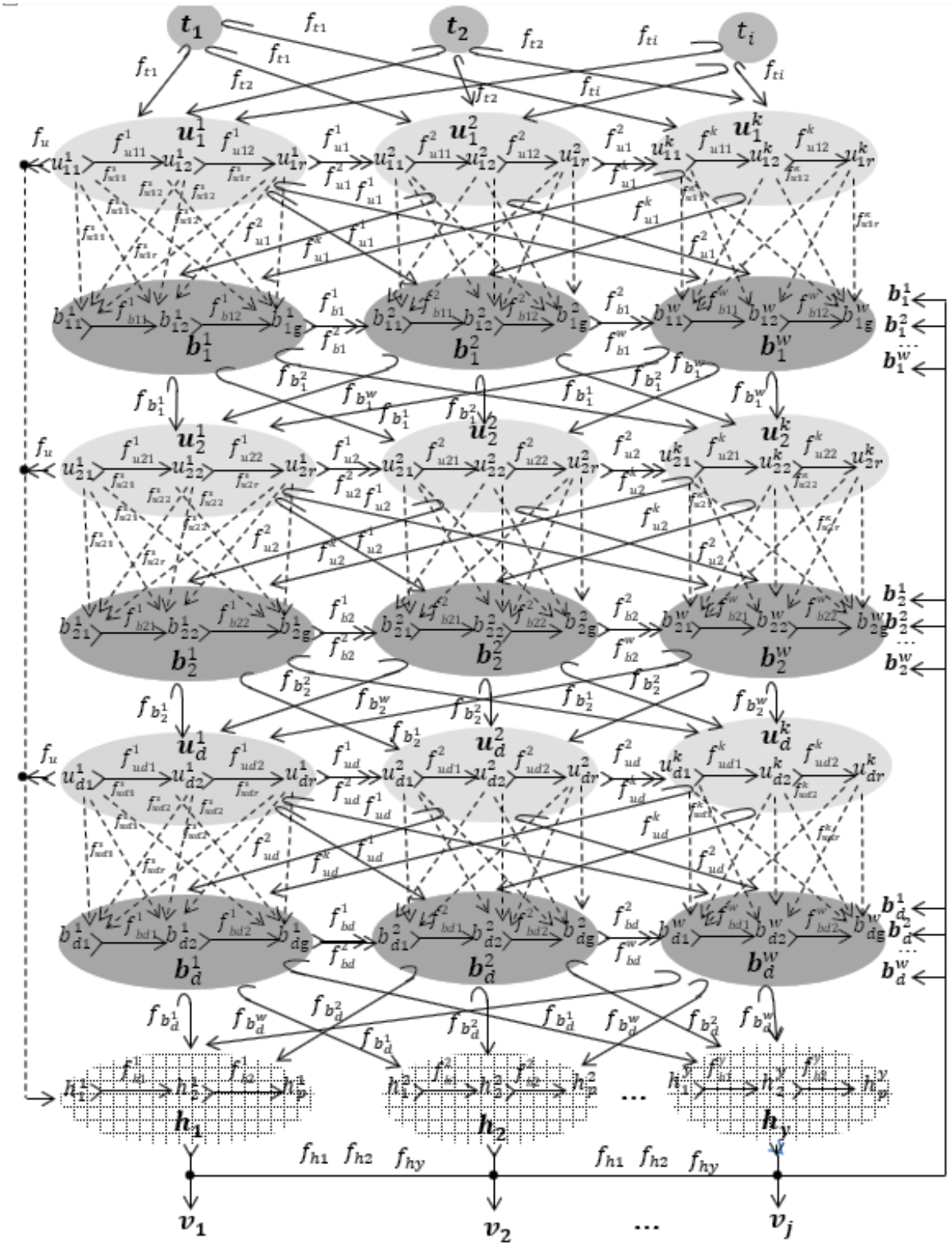

Рис. 8. Проєктна математична модель взаємовідносин множин загроз $t_1, t_2, \dots, t_i$ та множин системи захисту інформації: $u_1, u_2, \dots, u_d$ – уразливостей механізмів захисту, $b_1, b_2, \dots, b_d$ – бар'єрів захисту (фільтрів), $h_1, h_2, \dots, h_y$ – множини підсистеми аналізу загроз, $v_1, v_2, \dots, v_j$ – множини областей захисту інформаційної системи

Відношення еквівалентності на множині $\boldsymbol{H}$ по визначенню – відношення $R \subseteq \boldsymbol{H} \times A$ – має такі 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;

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

Процес ототожнення еквівалентних множин упроваджується в об'єднання цих множин в одну множину у разі поєднання їх одна з одною відношенням еквівалентності. Сукупності, які виникають, розглядаються тут як нові відношення. Формально для $a \in A$ визначається клас R-еквівалентності як множина: $[a] = \{b: aRb\}$ усіх елементів з A, які перебувають у R-відношенні до a.

Одна і та сама множина може бути класом еквівалентності різних елементів. У загальному випадку:

• $[a] = [b]$ тоді і тільки тоді, коли aRb. Тобто два еквівалентні елементи перебувають у відношенні R з однією і тією самою множиною елементів;

• якщо $[a] \neq [b]$, то $[a] \cap [b] = \emptyset$. Тобто два різні класи еквівалентності не мають загальних елементів;

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

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

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

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 проєктування з R до A, тобто тих, які задаються рівняннями

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

4. ВИСНОВОК

Математична модель проєктних відносин загроз і 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 з кращим урахуванням практичного застосування визначати загальний порядок побудови структури систем захисту інформації на етапі ескізного проєктування. Це є вхідні дані для системи автоматичного проєктування побудови систем захисту інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Аналіз систем та методів виявлення несанкціонованих вторгнень у комп'ютерні мережі. (2020, 16 червня). У В. В. Литвинов та ін. *Математичні машини і системи.* К., ІПММС НАН України, 2018. 1 (с. 31–40).

[2] Колодчак, О. М. (2012). Сучасні методи виявлення аномалій в системах виявлення вторгнень, *Вісник Національного ун-ту "Львівська політехніка". Комп'ютерні системи та мережі,* 745, 98–104.

[3] Даниленко, Д. О., Смірнов, О. А., Мелешко Є. В. (2012). Дослідження методів виявлення вторгнень в телекомунікаційні системи та мережі. *Системи озброєння і військова техніка.* Х., Харківський нац. ун-т Повітряних Сил ім. І. Кожедуба, 1, 92–100.

[4] Al-Sakib Khan Pathan (2014). *The State of the Art in Intrusion Prevention and Detection*. New York, Auerbach Public.

[5] Amrit Pal Singh, Manik Deep Singh (2014). Analysis of Host-Based and Network-Based Intrusion Detection System India. *J. Computer Network and Information Security*, 8, 41–47.

[6] Завада, А. А., Самчишин, О. В., Охрімчук В. В. (2012). Аналіз сучасних систем виявлення атак і запобігання вторгненням. *Інформаційні системи*, Житомир: зб. наук. пр. ЖВІ НАУ, т. 6, № 12, 97–106.

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

[8] Lawal, O. B. (2013). Analysis and Evaluation of Network-Based Intrusion Detectionand Prevention System in an Enterprise Network Using Snort Freeware. *African Journal of Computing & ICT*, Ibadan, vol. 6, no. 2, 169–184.

[9] Довбешко, С. В., Толюпа, С. В., Шестак, Я. В. (2019). Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак. *Сучасний захист інформації: наук.-техн. журн.*, 1, 56–62.

[10] Toliupa, S., Nakonechnyi, V., Uspenskyi O. (2020). Signature and statistical analyzers in the cyber attack detection system, Information technology and security. *Ukrainian research papers collection*, vol. 7, issue 1(12), 69–79.

[11] Толюпа, С., Штаненко, С., Берестовенко, Г. (2018). Класифікаційні ознаки систем виявлення атак та напрямки їх побудови: зб. наук. пр. Військового ін-ту телекомунікацій та інформатизації ім. Героїв Крут, вип. 3, 56–66.

[12] Toliupa, S., Druzhynin, V., Parkhomenko, I. Signature and statistical analyzers in the cyber attack detection system. *Scientific and Practical Cyber Security Journal (SPCSJ)*, 3(02), 47–53.

[13] Павлов, І. М., Хорошко В. О. (2013). Функторність та граничність відображень об'єктів множин в системах захисту інформації. *Інформаційна безпека*. К., 1(9),107–116.

[14] Павлов І. М. (2013). Альмагами, повнота діаграм та підоб'єкти множин в системах захисту інформації. *Інформатика та математичні методи в моделюванні*. ОНПІ, т. 3. № 1, 50–60.

REFERENCES

[1] Analysis of systems and methods for detecting unauthorized intrusions into computer networks. Retrieved June 16, 2020. In V. V. Litvinov [et al.], *Mathematical machines and systems.* K. IPMMS of the National Academy of Sciences of Ukraine, 2018. 1, 31–40 [in Ukrainian].

[2] Kolodchak, O. M. (2012). Modern methods of detecting anomalies in intrusion detection systems. *Bulletin of the Lviv Polytechnic National University. Computer systems and networks*, 745, 98–104 [in Ukrainian].

[3] Danylenko, D. O., Smirnov, O. A., Meleshko, E. V. (2012). Investigation of methods of detecting intrusions into telecommunication systems and networks. *Armament systems and military equipment.* H.: Hark. national Air Force University named after I. Kozheduba, 1, 92–100 [in Ukrainian].

[4] Al-Sakib Khan Pathan (2014). *The State of the Art in Intrusion Prevention and Detection*. New York, Auerbach Publications.

[5] Amrit Pal Singh, Manik Deep Singh (2014). Analysis of Host-Based and Network-Based Intrusion Detection System India. *J. Computer Network and Information Security*, vol. 8, 41–47.

[6] Zavada, A. A., Samchyshyn, O. V., Okhrimchuk, V. V. (2012). Analysis of modern systems for detecting attacks and preventing intrusions. *Information systems*, Zhytomyr: Collection of scientific works of ZhVI NAU, vol. 6, no. 12, 97–106 [in Ukrainian].

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

[8] Lawal, O. B. (2013). Analysis and Evaluation of Network-Based Intrusion Detectionand Prevention System in an Enterprise Network Using Snort Freeware. *African Journal of Computing & ICT*, Ibadan, vol. 6, no. 2, 169–184.

[9] Dovbeshko, S. V., Toliupa, S. V., Shestak, Y.V. (2019). Application of intelligent data analysis methods for building attack detection systems. *Scientific and Technical Journal "Modern Information Protection"*, no. 1, 56–62 [in Ukrainian].

[10] Toliupa, S., Nakonechnyi, V., Uspenskyi, O. (2020). Signature and statistical analyzers in the cyber attack detection system, Information technology and security. *Ukrainian research papers collection*, vol. 7, issue 1(12), 69–79.

[11] Toliupa, S., Shtanenko, S., Berestovenko, G. (2018). 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 Heroes Krut, issue 3, 56–66 [in Ukrainian].

[12] Toliupa, S., Druzhynin, V., Parkhomenko, I. Signature and statistical analyzers in the cyber attack detection system. *Scientific and Practical Cyber Security Journal (SPCSJ)*, 3(02), 47–53.

[13] Pavlov, I. M., Khoroshko, V. O. (2013). Functority and finiteness of mappings of set objects in information protection systems. *Information Security*. K., 1(9), 107–116 [in Ukrainian].

[14] Pavlov, I. M. (2013). Almagrams, completeness of diagrams and subobjects of sets in information protection systems. *Informatics and mathematical methods in modeling*. ONPI, vol. 3, no. 1, 50–60 [in Ukrainian].

Стаття надійшла до редколегії 08.03.2023

Mathematical model of system relationships management of information security

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.

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

Сергій Толюпа,
д-р техн. наук, проф.,
Професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка. Київ, Україна.

Serhii Toliupa,
Dr. Sci. (Engin.), Prof.
Professor of the Department of Cyber Security and Information Protection of Taras Shevchenko Kyiv National University. Kyiv, Ukraine.

Сергій Штаненко,
канд. техн. наук, доц.
Доцент кафедри побудови телекомунікаційних систем Військового інституту телекомунікацій та інформатизації імені Героїв Крут. Київ, Україна.

Serhii Shtanenko,
PhD (Engin.), Associate Prof.
Associate Professor of the Department construction of military telecommunication systems. Institute of Telecommunications and Informatization named after Heroes Krut. Kyiv, Ukraine