УДК 681.3.06

О.В. ПОТІЙ

Інститут інформаційних технологій, Україна

ФОРМАЛІЗОВАНА МОДЕЛЬ ДІЯЛЬНОСТІ ІЗ ЗАХИСТУ ІНФОРМАЦІЇ

Розглядається формалізована модель діяльності з захисту інформації, яка відображає макро- та мікроструктури діяльності із захисту інформації. Надані формальні конструкції макроструктури діяльності та мікроструктурі діяльності.

діяльність із захисту інформації, модель діяльності, безпека інформації

Вступ

Під час вирішення задач проектування комплексної системи захисту інформації (КСЗІ) в цілому та організаційної системи захисту інформації (ОСЗІ), як її складової частини, вимагається глибоке розуміння специфіки функціонування ОСЗІ, виконання аналізу умов здійснення захисту інформації та взаємодії з іншими підсистемами КСЗІ. Розробка моделі дозволяє перевірити різні аспекти функціонування ОСЗІ, дослідити вплив на систему зовнішніх факторів, оцінити ефективність у різних умовах функціонування. Модель дозволяє перевіряти ідеї, що висуваються під час розробки ОСЗІ, методи та засоби їх реалізації та оцінювати результат. Таким чином, побудова вірної моделі – це центральний етап проектування будь-якої системи і ОСЗІ не є виключенням.

Сьогодні перед керівником служби захисту інформації встають такі питання:

– які процеси захисту інформації потрібні для забезпечення рівня безпеки інформації, що вимагається?

– які відношення та зв'язки між процесами захисту інформації є суттєвими для забезпечення безпеки інформації?

– які технології необхідні для забезпечення інтеграції та впровадження заходів захисту інформації у повсякденну діяльність?

– які організаційні структури забезпечать ефективне виконання процесів захисту інформації та досягнення цілей безпеки?

Але відповідь на питання «що» необхідно організації, відразу же піднімає питання «як» та «де», наприклад:

– як розробити та реалізувати процеси захисту інформації, що забезпечують бажаний рівень безпеки інформації?

– яким чином швидко та ефективно впровадити технології, техніку та засоби захисту інформації у повсякденну практику захисту?

– які заходи захисту інформації потрібно реалізувати власними силами, а які – на основі аутсорсингу?

Відповідь на ці та багато інших питань пропонується отримати у рамках системодіяльнісної методології захисту інформації, а практична реалізація захисту інформації може здійснюватися на основі процесного підходу [1 – 4]. В рамках цієї методології під захистом інформації ми розуміємо систематичну, стабільну та цілеспрямовану діяльність суб'єкту захисту інформації (людини, організації, держави) відносно досягнення цілей захисту інформації та вирішення основних задач захисту інформації (забезпечення конфіденційності, доступності, цілісності та спостережливості інформації та систем), а також рівня довіри (гарантій), що вимагається. Під процесом захисту інформації будемо розуміти сукупність взаємопов'язаних операцій та дій, спрямованих на реалізацію комплексу заходів захисту інформації на основі визначеної технології (техніки) захисту шляхом перетворення вхідних матеріальних та інформаційних потоків у вихідні, що

представляють інтерес для суб'єкту захисту інформації. А під заходом захисту – політику (правила), процедури, дії, технології та організаційні структури, впроваджені суб'єктом захисту інформації у відношенні до об'єктів захисту (інформації, що захищається, інформаційної системи, об'єкту інформатизації тощо) з метою рішення основних задач захисту (забезпечення конфіденційності, цілісності, доступності та спостережності інформації та інформаційних систем), а також забезпечення гарантій (упевненості) у досягненні цілей захисту. Але на сьогоднішній день теоретичний та науково-методичній апарат процесного підходу до захисту інформації не є достатньо розвинутим та розробленим. Практика впровадження процесного підходу вимагає розроблення та використання різних моделей процесів захисту інформації, оскільки керівникам організації, керівникам підрозділів захисту інформації, офіцерам безпеки необхідна чітка картина діяльності із захисту інформації. У існуючий нормативній базі на цей час визначені лише сукупності заходів захисту інформації [5 – 10]. У міжнародному стандарті ISO/IEC 21827 [11] міститься перелік базових практик та сфер практичної діяльності із захисту інформації. Але стандарт не визначає структури процесів захисту інформації, не встановлює відношень між елементами діяльності. У роботі [12] запропонована формальна модель процесу захисту інформації, а у роботі [13] була зроблена спроба визначити еталонну модель процесів захисту інформації. У даній роботі вирішується задача теоретичного узагальнення результатів досліджень та розробки узагальненої формалізованої моделі діяльності, що у подальшому може використовуватися як основа для розробки структури діяльності із захисту інформації та як базис для проектування організаційної системи захисту інформації.

Модель діяльності як основа проектування організаційної системи захисту інформації

З точки зори розробки моделі діяльності нам потрібно вирішити дві задачі.

По-перше, під час аналізу діяльності із захисту інформації необхідно визначити та встановити склад та структуру цієї діяльності, тобто виявити інваріанти діяльності при всіх її перетвореннях, в залежності від особливостей тих або інших заходів захисту та від особливостей організаційної системи, в рамках якої здійснюється ця діяльність. Тому діяльність розглядається як система взаємодії суб'єктів діяльності з об'єктом діяльності.

По-друге. Діяльність із захисту інформації є складною діяльністю, яка містить різні операції, дії, роботи тощо. Тому важливим елементом аналізу діяльності є встановлення взаємозв'язків та взаємо залежностей між окремими операціями та діями, тобто встановлення певного типу відношень між ними.

Для встановлення структури діяльності з реалізації процесів пропонується застосовувати нормативний підхід. Суть нормативного підходу полягає у тому, що спираючись на вимоги нормативних документів щодо забезпечення безпеки інформації, емпіричні дані захисту інформації, ми будуємо нормативну структуру діяльності із захисту інформації, яка має цілеутворюючий чинник – забезпечення досягнення певних цілей захисту. Для цього структура діяльності формується таким чином, щоб відповідні операції та дії були спрямовані на вирішення задач захисту та отримання відповідних результатів. Подальше експериментальне здійснення такої діяльності конкретним суб'єктом дозволить встановити, наскільки теоретичні передумови, на основі яких була розроблена нормативна модель діяльності, були вірними, та чи є ця модель іманентною для будь-якого суб'єкту.

Для подальших міркувань уведемо до розгляду декілька визначень.

Визначення 1. Система процесів захисту інформації – це сукупність взаємопов'язаних та взаємодіючих процесів захисту інформації, що включають до себе всі види діяльності із захисту інформації, які можуть виконуватися в організації.

Взагалі пропонується виділити еталонну (ідеальну), нормативну, цільову та робочу системи процесів захисту інформації.

Визначення 2. Еталонна (ідеальна) система процесів захисту інформації S_E – це теоретично обґрунтована, несуперечлива та повна сукупність процесів захисту інформації, які можуть бути реалізовані будь-яким суб'єктом захисту інформації. Побудова еталонної моделі мабуть є задачею, яка не може бути вирішена у повному обсязі.

Визначення 3. Нормативна система процесів захисту інформації S_H – це сукупність процесів захисту інформації, яка побудована у відповідності до вимог одного або комплексу нормативних документів (стандартів).

Нормативна модель являє собою сукупність універсальних процесів захисту інформації, які є фундаментальними для забезпечення безпеки інформації та містять зразки передової практики захисту інформації, Нормативна модель, що наближається до еталонної (ідеальної) моделі, описує процеси, які організація (або організаційні підрозділи) може застосовувати для реалізації заходів захисту інформації, досягнення цілей та вирішення задач захисту. Основним призначенням нормативної моделі є формування загального базису для розроблення математичних та інших моделей та методів оцінювання ефективності захисту інформації, атестації процесів захисту інформації, проектування організаційної системи захисту інформації.

Визначення 4. Цільова система процесів захисту інформації $S_Ц$ – це сукупність процесів захисту інформації, які необхідно виконати в організації у відповідності до встановлених потреб, цілей та задач захисту.

Визначення 5. Робоча система процесів захисту інформації S_P – це сукупність процесів захисту інформації, яка містить всі види діяльності із захисту інформації, що здійснюються на даному підприємстві (організації) у поточний період.

Для даних систем процесів справедливо співвідношення

$$S_P \subseteq S_Ц \subseteq S_H \subseteq S_E .$$

Важливо підкреслити, що моделювання використовується під час проектування, створення, впровадження, експлуатації КСЗІ, а також на різних рівнях вивчення системи, починаючі від аналізу складових елементів КСЗІ та закінчуючи дослідженням КСЗІ у цілому в умовах її взаємодії із середовищем безпеки. Моделювання діяльності із захисту інформації пропонується здійснювати на макрорівні та мікрорівні. Формально модель діяльності пропонується представити у вигляді сукупності макро- та мікроструктури діяльності

$$NM_{SI} = \left\langle M_{SI}^{macro}, M_{SI}^{micro} \right\rangle . \qquad (1)$$

Макроструктура діяльності представляє собою структуру верхнього рівня та визначається множиною процесів захисту інформації і встановленими на цій множині відповідними відношеннями. Макроструктура – це по суті метамодель, яка характеризує процеси та їх взаємовідношення.

Мікроструктура діяльності розкриває внутрішню будову діяльності із захисту інформації, встановлює призначення кожного процесу та містить функціональну модель процесів захисту інформації.

Формалізована модель макроструктури діяльності із захисту інформації

Макроструктуру діяльності із захисту інформації будемо представляти конструкцією виду

$$M_{SI}^{macro} = \left\langle P, SC, V, D \right\rangle . \qquad (2)$$

Тут $P = \left\{ p_i \middle| i = \overline{1, I} \right\}$ – множина процесів захисту інформації; $SC = \left\{ sc_j \middle| j = \overline{1, J} \right\}$ – множина заходів захисту інформації; $V = V^{in} \cup V^{out}$ – повна множина вхідних та вихідних інформаційних та матеріальних артефактів діяльності із захисту інформації, де $V^{in} = \left\{ v_l^{in} \middle| l = \overline{1, L_{in}} \right\}$ та $V^{out} = \left\{ v_l^{out} \middle| l = \overline{1, L_{out}} \right\}$;

$D = \left(d_y \middle| y = \overline{1, Y}\right)$ – множина відношень між компонентами моделі.

Встановимо такі види відношень:

– $d_1(P, SC)$ – відношення типу «процес – захід захисту інформації». Кожний кортеж відношення d_1 встановлює конкретній процес $p_i \in P$, спрямований на впровадження заходу (заходів) захисту інформації $sc_j \in SC$;

– $d_2(P)$ – відношення типу «процес – процес». Кожний кортеж відношення d_2 визначає зв'язок між процесами $p_i \in P$ та $p_j \in P$, де $i, j = \overline{1, I}$.

– $d_3(P, V)$ – відношення типу «процес – артефакт діяльності», що визначає використання вхідних артефактів та формування вихідних артефактів під час реалізації процесів захисту інформації.

Формалізовано макроструктура діяльності із захисту інформації може бути описана шляхом завдання множин $\{P, SC, V\}$ та булевих матриць суміжностей виду

$$PSC = \left\| psc_{ij} \right\|, \; P = \left\| p_{ij} \right\|, \; PV = \left\| pv_{il} \right\|, \qquad (3)$$

які задають відповідні відношення D між компонентами макроструктури. Елементи цих матриць дорівнюють одинці, якщо між відповідними компонентами є відношення (взаємозв'язок), та нулю у іншому випадку. Для візуалізації макроструктури доцільно також надавати її опис у вигляді відповідних графів. Так матриця $P = \left\| p_{ij} \right\|$ може бути представлена у вигляді графу $G = \left\langle p_i, a_{ij} \right\rangle$, де $p_i \in P$ – вершини графу; $a_{ij} \in A$ – ребра графу, що поєднують вершину p_i з вершиною p_j.

Вихідними даними для формування макроструктури діяльності є результати аналізу вимог стандартів та інших нормативних документів, обстежень та аудиту безпеки об'єктів інформаційної діяльності, які можуть бути представлені у відповідних формах та звітах.

Формалізована модель мікроструктури діяльності із захисту інформації

Формалізована модель мікроструктури діяльності із захисту інформації пропонується представляти у вигляді такої формальної конструкції

$$M_{SI}^{micro} = \left\langle M_{ПО}, M_{ЦП}, G_{П}, M_{ЦР}, M_{Ф} \right\rangle, \qquad (4)$$

де $M_{ПО}$ – модель предметної області родини процесів захисту інформації; $M_{ЦП}$ – модель типу «ціль-процес» (ЦП-модель), що відображає взаємозв'язок між цілями та процесами; $G_{П}$ – ієрархічна модель процесів (операцій, дій) захисту інформації; $M_{ЦР}$ – модель типу «ціль-результат» (ЦР-модель), що відображає взаємозв'язок між цілями та результатами захисту інформації; $M_{Ф}$ – функціональна модель процесів захисту інформації.

Модель предметної області родини процесів ЗІ будується для уточнення призначення процесів захисту інформації. Вона впливає на формування погляду дослідника на призначення ПЗІ, на загальну концепцію їх побудови та використання.

Модель предметної області родини процесів ЗІ представляє собою формальну конструкцію виду

$$M_{ПО} = \left\langle C; D(C); F(C, D) \right\rangle, \qquad (5)$$

де $C = \left\{ c_i \middle| i = \overline{1, I} \right\}$ – множина понять-концептів, що описують предметну область процесів ЗІ; $D(C) = \left\{ d_y \middle| y = \overline{1, Y} \right\}$ – множина відношень між концептами; $F(C, D)$ – відображення, що задає зв'язки між концептами та відношеннями. Відображення представляється у вигляді графу.

Модель предметної області процесу описується шляхом визначення множини концептів C та встановлення на цій множині відношень d_i.

Результати моделювання представляються у вигляді сукупності так званих інформаційно-понятійних діаграм. Модель дозволяє більш точніше визначити призначення процесів захисту інформації.

Модель типу «ціль-процес» (ЦП-модель) призначена для визначення сукупності взаємопов'язаних цілей захисту інформації та відповідних процесів (функцій), яки реалізуються для досягнення цих цілей. Ціль – це бажаний майбутній стан організаційної системи захисту інформації, який може бути досягнуто за рахунок виконання (реалізації) виділеної множини процесів (операцій та дій) з урахуванням критичних факторів успіху. Ціль – це суб'єктивна конструкція, що залежить від знань та суб'єктивних якостей аналітика. ЦП-модель є формальною конструкцією виду

$$M_{ЦП} = \langle P, Tar, D(P,Tar), G(Tar), F(P,Tar) \rangle . \quad (6)$$

Тут $P = \{p_i | i = \overline{1,I}\}$ – множина процесів, що входять до області визначення родини процесів; $Tar = \{tar_k | k = \overline{1,K}\}$ – множина цілей захисту інформації; $D(P,Tar)$ – відношення типу «підтримує», що встановлює конкретний процес (процеси); $p_i \in P$ – спрямований на досягнення (підтримку) конкретної цілі (цілей) захисту інформації $tar_k \in Tar$; $F(P,Tar)$ – відображення, що задає зв'язки між елементами множин P та Tar; $G(Tar)$ – деревоподібна ієрархія цілей. Деревоподібна ієрархія цілей представляється у вигляді орієнтованого графу без циклів, петель, горизонтальних ребер у границях одного рівня ієрархії виду

$$G(Tar) = \langle Tar, A \rangle , \quad (7)$$

де $Tar = \{tar_k | k = \overline{1,K}\}$ – множина вершин-цілей, $A = \{a_{ij}^n\}, i.j = \overline{1,K}$ – множина дуг, що з'єднують *i*-у вершину *n* рівня з *j*-ю вершиною *n*+1 рівня ієрархії. Тобто в графі $G(Tar)$ початку дуги відповідає вершина верхнього рівня ієрархії, а кінцю – вершина найближчого нижчого рівня ієрархії. Ребра графу відображають відношення підпорядкованості між цілями, що знаходяться на суміжних рівнях ієрархії.

Формалізовано модель описується шляхом завдання множини цілей захисту Tar та множини процесів захисту інформації P та встановлення на елементах відношення $D(P,Tar)$. Модель представляється у вигляді графу, що будується на основі ієрархії $G(Tar)$.

Ієрархічна модель процесів, або дерево процесів призначена для опису процесів з різним рівнем деталізації. При цьому процеси не представляються у хронологічному порядку. Дерево процесів представляється у вигляді орієнтованого графу без циклів, петель, горизонтальних ребер у границях одного рівня ієрархії виду

$$G_{П} = \langle P, A, D(P) \rangle , \quad (8)$$

де $P = \{p_i | i = \overline{1,I}\}$ – множина процесів, що входять до області визначення родини процесів; $A = \{a_{ij}^n\}, i.j = \overline{1,I}$ – множина дуг, що з'єднують *i*-у вершину *n* рівня з *j*-ю вершиною *n*+1 рівня ієрархії; $D(P) = \{d_{EOS}, d_{OOS}, d_{POS}\}$ – відношення підпорядкованості процесів. Кожний кортеж відношення d визначає тип підпорядкованості між процесами $p_i \in P$ та $p_j \in P$, де $i, j = \overline{1,I}$. Будемо розглядати таки типи відношень:

– $d_{EOS}(p_i, p_j)$ – відношення підпорядкованості за способом виконання, що відображає операційно-орієнтовний критерій об'єднання процесів (виконання однакових операцій);

– $d_{OOS}(p_i, p_j)$ – відношення підпорядкованості за об'єктом, що відображає об'єктно-орієнтовний критерій об'єднання процесів (обробка одного і того ж об'єкту);

– $d_{POS}(p_i, p_j)$ – відношення підпорядкованості за процесом, що відображає процесно-орієнтований критерій об'єднання процесів (приналежність одному і тому ж процесу).

Модель типу «ціль – результат» (ЦР-модель) призначена для відображення взаємозв'язку між цілями та результатами реалізації процесів, а також для представлення результатів у вигляді складових частин. Результатом процесу може бути продукт або

послуга, в яких зацікавлені учасники процесу. ЦР-модель представляє собою формальну конструкцію вигляду

$$M_{ЦР} = \langle Tar, Z, D, F(Tar, Z) \rangle . \quad (9)$$

Тут $Tar = \{ tar_k \,|\, k = \overline{1, K} \}$ – множина цілей захисту інформації; $Z = \{ z_m \,|\, m = \overline{1, M} \}$ – множина продуктів/послуг, що формуються як результат реалізації процесу захисту інформації; $D = \left(d_y \,|\, y = \overline{1, Y} \right)$ – множина відношень між компонентами моделі. Встановимо таки типи відношень:

– $d_1(Z, Tar)$ – відношення типу «підтримує». Відношення встановлює, що конкретний результат $z_m \in Z$ підтримує конкретну ціль захисту інформації $tar_k \in Tar$;

– $d_2(Z)$ – відношення типу «відноситься до групи». Відношення вказує, що результат $z_m \in Z$ відноситься до визначеної групи результатів.

ЦР-модель задається шляхом визначення множин $\{Tar, Z\}$, встановлення на цих множинах відповідних відношень D і представлення у вигляді діаграми (графу) $F(Tar, Z)$. ЦР-модель будується для уточнення призначення процесу, що є складовою частиною формальної моделі процесу [12].

Функціональна модель процесу відображає структуру процесів захисту інформації, а також потоки інформації та матеріальних об’єктів, що пов'язують ці процеси. Необхідність застосування методології функціонального моделювання викликана ускладненням систем захисту інформації (як організаційної, так і технічної складових) та необхідністю аналізу процесів захисту інформації (з системних позицій) з метою удосконалення функціонування та підвищення ефективності КСЗІ.

Формалізовано функціональну модель процесу можна представити у вигляді конструкції

$$M_{Ф} = \langle P, V, D(P), F(P) \rangle . \quad (10)$$

Тут $P = \{ p_i \,|\, i = \overline{1, I} \}$ – множина процесів захисту інформації; $V = V^{in} \cup V^{out}$ – повна множина вхідних та вихідних інформаційних та матеріальних артефактів діяльності із захисту інформації, де $V^{in} = \{ v_l^{in} \,|\, l = \overline{1, L_{in}} \}$ та $V^{out} = \{ v_l^{out} \,|\, l = \overline{1, L_{out}} \}$; $D(P)$ – множина відношень між компонентами моделі; $F(P)$ – відображення, що задає зв’язки між елементами множин P.

Для побудови функціональних моделей обрана методологія функціонального моделювання IDEF0 [14]. У відповідності до цієї методології встановлюються таки типи відношень: $d_{dom}(p_i, p_j)$ – відношення домінування, що характеризує вплив процесу p_i на процес p_j; $d_{man}(p_i, p_j)$ – відношення управління, яке відображає, що вихід v_i^{out} процесу p_i є управлінням (тобто є інформацією управління) для процесу p_j; $d_{io}(p_i, p_j)$ – відношення типу «вихід-вхід», яке відображає, що вихід v_i^{out} процесу p_i є входом v_j^{in} для процесу p_j; $d_{oif}(p_i, p_j)$ – відношення типу «зворотній зв'язок за входом», яке відображає, що вихід v_j^{out} процесу p_j спрямований на вхід v_i^{in} для процесу p_i. При цьому процес p_i домінує над процесом p_j; $d_{ocf}(p_i, p_j)$ – відношення типу «зворотній зв'язок за управлінням», яке відображає, що вихід v_j^{out} процесу p_j є управлінням для процесу p_i. При цьому процес p_i домінує над процесом p_j; $d_{om}(p_i, p_j)$ – відношення типу «вихід – механізм», яке відображає, що вихід v_i^{out} процесу p_i є механізмом для виконання процесу p_j.

Функціональна модель задається шляхом визначення множин $\{P, V\}$, встановлення на множині процесів відповідних відношень D. Для візуалізації моделі доцільно використовувати методологію функціонального моделювання IDEF0 [14].

Висновки

Запропонована сукупність формальних моделей структури діяльності із захисту інформації є теоретичним узагальненням практики захисту. Ці моделі використовується як теоретична основа для розробки нормативної, цільової та робочих моделей діяльності із захисту інформації, а також для визначення макро- та мікроструктури діяльності. Шляхом завдання всіх елементів розглянутих вище конструкцій можна конкретизувати склад та структуру діяльності із захисту інформації. У наступних публікаціях буде розглянута процедура розробки нормативної моделі діяльності із застосуванням нормативного підходу та надані результати моделювання процесів захисту інформації на основі використання методології SADT та методів функціонального моделювання IDEF0 та ARIS.

Формалізована модель, що пропонується у цій роботі, розроблена вперше та представляє собою нові знання відносно структури діяльності із захисту інформації. Результати, що отримані в цій роботі, носять теоретичний характер та можуть використовуватися на практиці для визначення організаційної системи захисту інформації. Запропонована модель є елементом теоретичних основ процесного підходу до захисту інформації.

Література

1. Бондаренко М.Ф., Потий О.В. Визначення та обґрунтування суті політики інформаційної безпеки // Радиотехника. – 2003. – Вып. 134. – С. 9-25.

2. Потій О.В. Процесний підхід до управління безпекою інформації // VIII Международная научно-практическая конференция"Безопасность информации в информационно-телекоммуникационных системах", 11-13 мая 2005. Тезисы докладов. – К.: НИЦ "Тезис", 2005. – С. 35-36.

3. Потій О.В., Леншин А.В. Методичні аспекти оцінки зрілості процесів захисту інформації в умовах невизначеності // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. – 2006. – Т.5, №1. – С. 134-138.

4. Потий А.В., Ларгин И.В., Ткачук Ю.П. Описание требований безопасности информации в нотации ARIS eEPC // Радіоелектронні і комп'ютерні системи. – 2006. – № 6. – С. 75-80.

5. ISO/IEC 17779:2000 Code of practice for information security management.

6. NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems 7. Bundesamt fur Sicherheit in der Informationstechnik. IT Baseline Protection Manual, 1998.

8. ДСТУ ISO/IEC TR 13335-2:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 2: Керування та планування безпеки інформаційних технологій.

9. ISO/IEC 27001:2005 (BS 7799-2:2005) Information technology Security techniques – Information Security Management Systems.

10. NIST SP 800-53. Recommended Security Controls for Federal Information Systems / R.Ross, S. Katzke, A. Johnson, M. Swanson, G. Stoneburner, G. Rogers, A. Lee. – 2005.

11. ISO/IEC 21827: 2002 Information technology – Systems Security Engineering – Capability Maturity Model.

12. Потий А.В. Формальная модель процесса защиты информации // Радіоелектронні і комп'ютерні системи. – 2006. – № 5. – С. 75-80.

13. Потий А.В. Эталонная модель системы процессов защиты информации // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К.; 2006. – Вип.12. – С. 17-31.

14. РД IDEF 0. Методология функционального моделирования IDEF0. Руководящий документ. – Госстандарт России, Москва, 2000.

Надійшла до редакції 30.01.2007

Рецензент: д-р техн. наук, проф. В.І. Долгов, Харківський національний університет радіоелектроніки, Харків.