УДК 004.415.056.5(075)

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 3, pp. 263-271

МЕТОДОЛОГІЯ ОБҐРУНТУВАННЯ ОСНОВНИХ ЗАГАЛЬНОСИСТЕМНИХ ВИМОГ ДО ПРОЕКТУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

І.М. Павлов

Державний університет телекомунікацій,
вул. Солом'янська, 7, Київ, 03680, Україна; e-mail: pavlov@ukr.net

У статті пропонуються методики у складі методології обґрунтування основних загальносистемних вимог до проектування систем захисту інформації на основі методів групового врахування аргументів, аналогій, експертного оцінювання та статистичного оброблення даних.

Ключові слова: вимоги, властивості, методологія, методики, система захисту інформації.

Постановка проблеми

Визначити напрями розвитку систем захисту інформації можливо лише після обґрунтування основних загальносистемних вимог на основі сучасної методичної бази [1-5]. Аналіз сучасного стану методичного апарату обґрунтування вимог до систем захисту інформації свідчить, що його основним недоліком є використання виключно внутрішніх властивостей системи захисту інформації, без врахування їх «внеску» до систем вищого рівня – інформаційних систем (ІС), а також ототожнення методик оцінювання систем захисту інформації з методиками обґрунтування вимог до них. Крім того, на об'єктах критичної інфраструктури (ОКІ) робота ІС тісно пов'язана зі специфікою цих об'єктів, що накладає особливості на вимоги до систем захисту інформації, як систем критичного застосування цих об'єктів.

У зв'язку з цим, розроблення підходу, який надав би змогу уникнути зазначених недоліків та обґрунтувати основні загальносистемні вимоги до систем захисту інформації, є актуальним науковим завданням.

Аналіз останніх досліджень і публікацій

Аналіз останніх публікацій дає змогу дійти висновку, що сучасні методичні підходи розрізнені й специфічні щодо способу обґрунтування загальносистемних вимог до систем захисту інформації (СЗІ) та мають ряд принципових недоліків. Так, використання методичного підходу [3] дає змогу обґрунтувати лише наближені значення основних вимог до СЗІ, оскільки в ньому для визначення ефективності захисту використовується ряд величин, що важко піддаються формалізації. До таких величин належать гравітаційна модель, яка використовує одиницю ефективності засобів захисту з системи обмежень задач. Методики [4,5] за своєю суттю є оцінювальними, оскільки вхідними даними в них є часткові показники внутрішніх властивостей СЗІ, а не показники систем більш високого порядку (відповідно до ІС у

цілому). В результаті використання таких методик можна дійти висновку лише про відповідність СЗІ «директивно встановленим» вимогам.

Таким чином, *метою* статті є обґрунтування основних загальносистемних вимог до проектування систем захисту інформації на ОКІ.

Основна частина

На початку XXI століття не лише багато зарубіжних країн, а й терористичні і кримінальні структури інтенсивно вдосконалюють методи та способи використання інформаційних технологій і засобів деструктивних впливів на інформаційні ресурси державних, комерційних підприємств та організацій. Таке застосування інформаційних технологій і засобів надає таким застосуванням властивості інформаційної зброї, яка може бути застосована в будь-який час.

З огляду на такі тенденції в більшості країн світу з метою систематизації об'єктів, втрата або порушення нормального функціонування яких призведе до значних або непоправних негативних наслідків для національної безпеки, введено поняття «критична інфраструктура», основою яких є системи критичного застосування [6].

Особливістю систем критичного застосування є те, що інформаційна безпека традиційно зосереджена на досягненні наступних цілей: конфіденційності, цілісності, доступності. Стратегія безпеки традиційної інформаційної технології спрямована, в першу чергу, на конфіденційність із необхідними засобами управління доступом для досягнення заданої мети. Безпека в цих системах стосується підтримки доступності всіх компонентів системи. При цьому, цілісність є часто другою за важливістю задачею.

Задачі забезпечення основних функцій ІС критичного застосування іноді входять всупереч із задачами їх інформаційної безпеки. Це викликано тим, що критичні інфраструктури мають особливості, які суттєво впливають на зміст вимог щодо забезпечення захисту інформації, а саме [7]: наряду з широким застосуванням систем, які мають операційні системи, працюючі в режимі реального часу, ускладненого взаємозв'язку інформаційного захисту з фізичними процесами і наслідками в промисловому секторі – основними видами інформації, що захищається в ІС критичного застосування, є технологічна (забезпечує управління технологіями або чутливо важливими процесами), програмно-технічна (програми системного і прикладного характеру, що забезпечують функціонування об'єктів), командна (управлінська) і вимірювальна, які не належать до інформації з обмеженим доступом (якщо в таких системах циркулює інформація з обмеженим доступом, то вона підлягає захисту згідно з чинними вимогами і нормами технічного захисту інформації).

Враховуючи зазначене, для вирішення питань розглянемо процес захисту інформації, з одного боку, як об'єкт, що містить інші підсистеми, а з іншого – як елемент ІС більш високого порядку.

Загальна структура запропонованої методики (рис. 1) складається з чотирьох основних блоків: блок 1 – формування вихідних даних; блок 2 – визначення системи показників; блок 3 – формування обмежень; блок 4 – розрахунок значень показників основних загальносистемних вимог до СЗІ; блок 5 – визначення рекомендацій.

Вихідними даними для методології визначення основних вимог до СЗІ на ОКІ є (блок 1): показник ефективності захисту інформації в системі критичного застосування, який задається; варіанти типових СЗІ критичного застосування за результатами досліджень; зовнішні та внутрішні фактори впливу на захист інформації в системах критичного застосування; параметри ІС ОКІ. Під показниками СЗІ (блок 2) визначаються властивості СЗІ та задачі, які необхідно розглядати СЗІ.

У таблиці 1 наведені властивості СЗІ як складних ІС (додатково розширений перелік з [8]). Зрозуміло, що цей перелік не є вичерпаним і повинен бути розширеним. Однак вже з його аналізу видно, що умовно властивості СЗІ можна поділити на

незалежні та взаємопов'язані. Тому доцільно побудувати ієрархію необхідних властивостей та визначити відносну важливість кожної властивості. Найменш важливі властивості можуть бути виключені з подальшого розгляду.

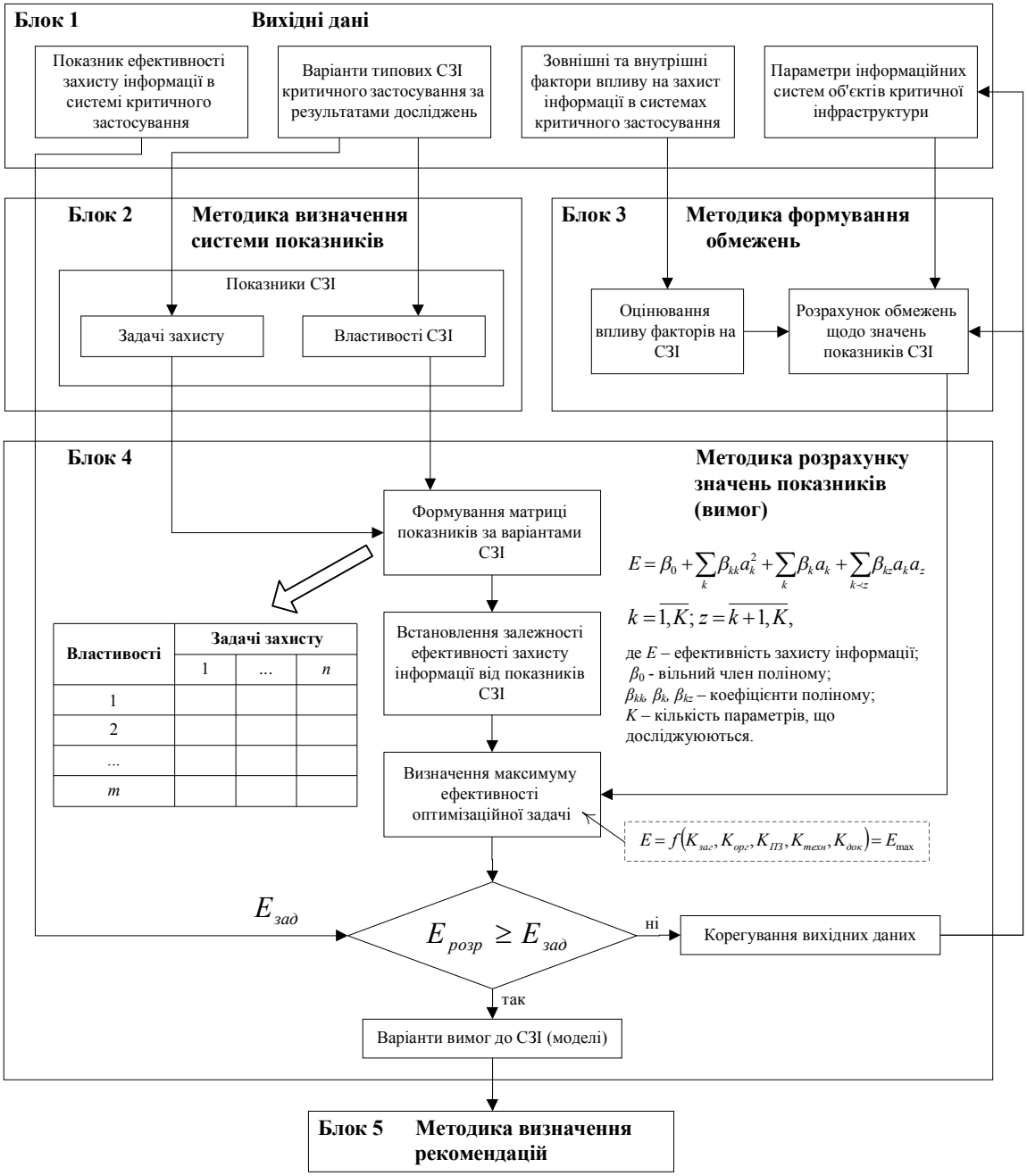

Рис. 1. Загальна структура методології обґрунтування основних загальносистемних вимог до проектування систем захисту інформації ОКІ

У подальшому для кожної властивості (з тих, які залишились) необхідно визначити сукупність показників, які її характеризують, їх відносну важливість стосовно той або іншої властивості, можливий діапазон їх зміни, а також градації значень показників, які відповідають обраній шкалі якості (наприклад, трирівнева шкала: висока, середня, низька). Після цього доцільно визначити важливість кожного показника відносно усієї сукупності показників та найменш важливі з них виключити з подальшого розгляду.

Таблиця 1.

Властивості систем захисту інформації як складних інформаційних систем

Автономність роботи	Адекватність	Безпечність
Здатність до взаємодії	Взаємозамінність	Відновлюваність
Відповідність	Відстежуваність	Придатність до встановлення або монтажу
Гнучкість	Готовність до негайного використання	Деградованість
Довговічність	Доступність за можливістю використання	Доступність за ціною
Експлуатаційна придатність	Ергономічність	Ефективність щодо виконання процесу
Ефективність щодо планування	Живучість	Спроможність виконання критеріїв захисту інформації (конфіденційність, цілісність, доступність, спостережність)
Змінюваність	Інтегрованість	Конструктивність
Придатність до зміни конфігурації	Легальність	Масштабованість
Мобільність	Придатність до модернізації	Придатність до модифікації
Модульність	Надійність	Налаштованість
Аудит	Повторюваність	Працездатність
Пристосованість	Прогнозованість	Простота побудови та використання
Ремонтопридатність	Придатність до негайного розгортання	Розширюваність
Стабільність	Стандартизованість	Стійкість
Сумісність	Тестованість	Точність
Транспортабельність	Універсальність	Чутливість

Окрім того, усі показники доцільно поділити на 2 групи: які не є джерелом протиріч між властивостями, та показники, кращі значення яких для одних властивостей мають наслідком погіршення деяких інших властивостей. Для показників першої групи можна одразу висунути вимогу щодо належності їх значень до діапазону, який відповідає високій якості відповідних властивостей. Показники другої групи вимагають більш детального аналізу та прийняття компромісних рішень щодо їх значень для забезпечення прийнятої якості властивостей, на які вони впливають.

Необхідно зазначити, що формально можуть існувати деякі специфічні показники, що характеризують систему, але які складно віднести до деякої властивості. До таких показників діапазон зміни їх значень доцільно поділити на інтервали, які відповідають обраній шкалі якості самої ІС та висунути вимогу щодо належності їх значень, які реалізуються, діапазону, який відповідає високій якості системи.

Для розрахунку значень та формування матриці показників за варіантами вимог до системи захисту об'єкта $w_i \in W$, $i = \overline{1,n}$, і до процедур над нею, сформулюємо задачі, які припускають оптимізацію по всіх елементах [9]: $M_\tau(w_i) \subseteq M(w_i), \tau = \overline{1,\sigma}$.

Задача 1. Мінімізація вартості забезпечення захисту об'єкта $w_i \in W$, $i = \overline{1,n}$, тобто $S(w_i) = \sum_{j=1}^{k} S_j(w_i)\chi^j(w_i) \to \min_{M_\tau(w_i)}, \tau = \overline{1,\sigma}$ при наступних обмеженнях: $\sum_{j=1}^{k} \chi_\tau^j(w_i) \le k$, $\sum_{j\in J} I_j(w_i)\chi_\tau^j(w_i) \ge J_0(w_i)$, $\sum_{j=1}^{k} S_j(w_i)\chi_\tau^j(w_i) \le S_0(w_i)$, $\chi_\tau^j(w_i) = 1 \vee 0$.

Більш точно задача формується з урахуванням нерівності, яку можна розрахувати з умовою: вартість захисту об'єкта повинна бути мінімізована, принаймні, вона не повинна перевищувати певної величини, скажемо $S(w_i)$:

$$S(w_i) = \sum_{j=1}^{k} S_j^n(w_i)\chi^j(w_i) + \max_{i\in 1} T_0(w_i)\sum_{j=1}^{k} S_j^\ni(w_i)\chi^j(w_i) = S^n(w_i) + \max_{i\in 1} T_0(w_i)S^\ni(w_i) \le S_0(w_i),$$

$w_i \in W$, $i = \overline{1,n}$, тобто з роздільним обліком вартості проектування і експлуатації засобів і методів, застосованих для захисту об'єкта.

Задача 2. Мінімізація ефективності систем захисту об'єкта $w_i \in W : v(w_i) - S(w_i) \to \max_{M_\tau(w_i)}$, при обмеженнях задачі 1.

Задача 3. Мінімізація ймовірності злому всіх методів, які використовуються для захисту об'єкта, при обмеженнях, прийнятих при розв'язку задач 1 і 2: $P(w_i) = 1 - \prod_{j=1}^{k}\left(1 - p_j(w_i)\right)\chi^j \to \min_{M_\tau(w_i)}$.

Задача 4. Максимізація вартості злому усіх методів, які використовуються для захисту об'єкта $w_i \in W$: $C(w_i) = \sum_{j=1}^{k} c_j(w_i)p_j(w_i)\chi^j(w_i) \to \max_{M_\tau(w_i)}$, при обмеженнях задачі 1, а також наступних: $\sum_{j=1}^{k} t_j p_j(w_i)\chi^j(w_i) \ge T_0(w_i)$, $\sum_{j=1}^{k} c_j(w_i)p_j(w_i)\chi^j(w_i) \succ v(w_i)$.

Задача 5. Мінімізація величини втрат від злому всіх методів, які використовуються для захисту об'єкта $w_i \in W$: $\pi(w_i) = \sum_{j=1}^{k} \pi_j(w_i)p_j(w_i)\chi^j(w_i) \to \min_{M_\tau(w_i)}$, при обмеженнях, прийнятих у задачі 4, а також обмеження на вартість злому системи захисту об'єкта: $\sum_{j=1}^{k} \pi_j(w_i)p_j(w_i)\chi^j(w_i) \prec c_0(w_i)$.

Розв'язок зазначених задач дозволить сформувати кращу матрицю за варіантами СЗІ, а розв'язок відповідної сукупності задач для всієї множини об'єктів W - створити сукупність загальносистемних підходів до побудови варіанту СЗІ для системи в цілому.

Основне призначення блока 3 – це формування обмежень на основі врахування зовнішніх і внутрішніх факторів впливу на інформацію та СЗІ. Схематично методика формування обмежень для визначення вимог до СЗІ ОКІ наведена на рис. 2.

Причиною уразливості ОКІ можуть бути недоліки або слабкі місця ІС, захисту інформації, процедур внутрішнього контролю, які можуть бути використані з метою порушення процедур безпеки інформації. Основні зовнішні і внутрішні фактори, які впливають на захист інформації в ОКІ, представлені на рис. 3.

Сукупність вимог до СЗІ докладно представлено в [10]. У загальному випадку доцільно виділити наступні групи вимог до СЗІ: загальні, організаційні, конкретні вимоги до підсистем захисту, технічного і програмного забезпечення, документування, способів і методів захисту. У подальшому проводиться розрахунок обмежень щодо показників СЗІ. Загальний підхід до методики розрахунку значень показників (вимог) (блок 4) наданий на рис. 1.

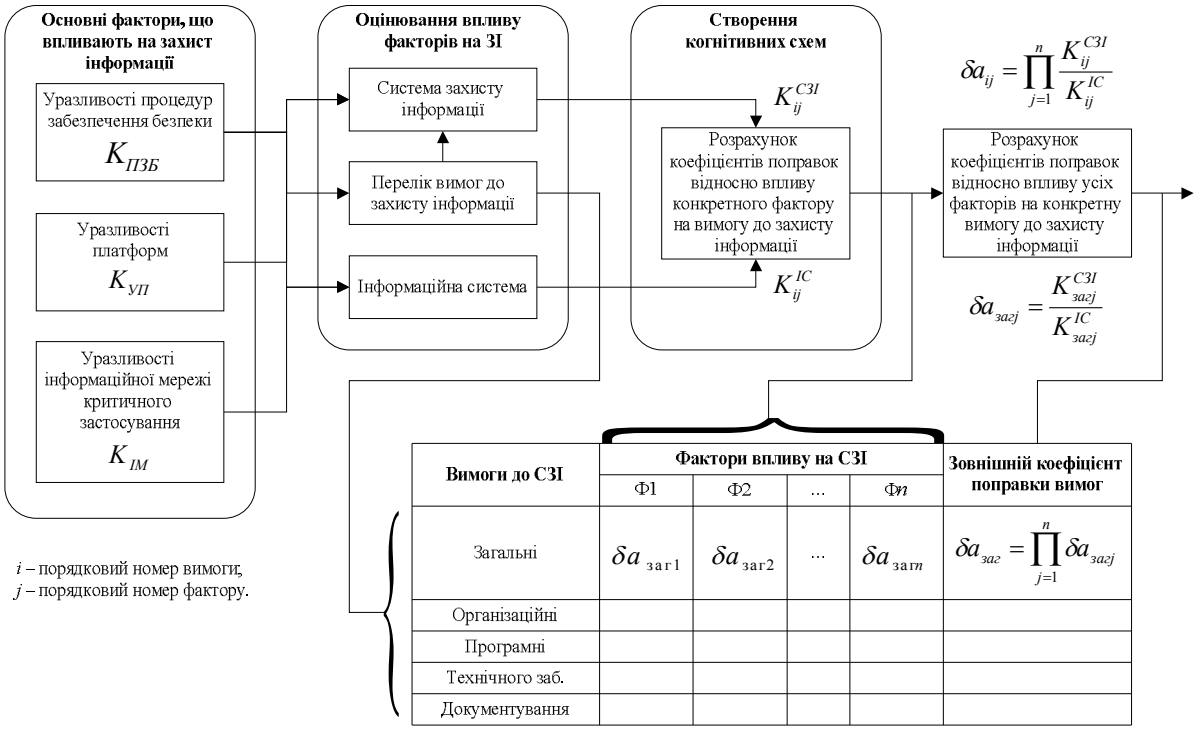

Рис. 2. Методика формування обмежень для визначення вимог до систем захисту інформації ОКІ

Для визначення кінцевого варіанту загальносистемних вимог до СЗІ, які отримані під час розрахунків у блоці 4, необхідно оцінити обґрунтованість рекомендацій, які необхідно прийняти для визначення структури СЗІ на основі багатокритеріального порівняння альтернативних варіантів СЗІ (блок 5), для чого пропонується методика обґрунтування рекомендацій. Як показник обґрунтованості пропонується використовувати ймовірність p_0 того, що альтернативні варіанти СЗІ дійсно є кращими. Відповідно, критерій обґрунтованості має вигляд $p_0 \geq p_z$, де p_z – мінімально припустиме значення ймовірності того, що рекомендовані вимоги до СЗІ дійсно є кращими. Показник p_0 визначається через ймовірність трьох незалежних подій: модель функціонування СЗІ, з використанням якої формується множина альтернативних варіантів, є адекватною; найкращий варіант системи потрапив до переліку порівнювальних альтернатив; з переліку альтернатив методами багато вимірювального порівняльного аналізу були відібрані дійсно найкращі варіанти СЗІ. Тоді критерій обґрунтованості набуває вигляду $p_0 = p_1 p_2 p_3 \geq p_z$, де p_1, p_2, p_3 – ймовірності першої, другої та третьої події відповідно.

Значення показників p_1, p_2, p_3 можна обчислити. Якщо модель функціонування СЗІ отримана на основі методів планування експерименту [11], то ймовірність першої події дорівнює довірчій ймовірності, для значення якої була оцінена адекватність регресійної моделі (зазвичай, 0.9-0.95), тобто p_1=0.90-0.95.

Якщо безпосередньо оцінити адекватність моделі неможливо, тоді доцільно скористатися експертним оцінюванням величини p_1 відповідно до підходу, наведеному в [12], тобто запропонувати експерту надати вербальну оцінку своєї впевненості в адекватності використаної моделі, а потім перевести отриману вербальну оцінку в числову відповідно до співвідношень, які наведені в таблиці 2.

Уразливості процедур забезпечення безпеки
- невідповідність або відсутність процедур забезпечення безпеки; - відсутність підвищення кваліфікації персоналу; - невідповідність архітектури безпеки; - невідповідність або відсутність керівництва з впровадження обладнання; - відсутність відповідальності за адміністрування безпеки; - відсутність або недоліки аудитів в сфері безпеки; - відсутність конкретного плану аварійного відновлення системи у разі збою або аварії; - відсутність змін конфігурації управління.
Уразливості платформ інформаційних систем критичного застосування
- *конфігурація:* ПЗ не оновлюється; ОС та програми безпеки використовуються без випробувань;параметри використовуються за замовчуванням; не зберігаються критичні конфігурації; зберігання незахищених конфігурації даних (паролів і т.п.); - *обладнання:* невідповідне тестування змін системи безпеки; недостатній рівень фізичного захисту; НСД до обладнання; незахищений відділений доступ; подвійні мережеві карти; відсутність документування активів; радіочастотний і електромагнітний імпульси; відсутність резервного електроживлення; втрата контролю навколишнього середовища; відсутність резервування критично важливих компонентів; - *програмне забезпечення:* переповнення буферу; відмова в обслуговуванні; неправильна обробка невизначених, погано визначених або «неприпустимих» умов; використання незахищених протоколів ПД; передача повідомлень в незахищеному вигляді; запуск надлишкових серверів; недостатня перевірка справжності та контролю доступу; відсутність програм безпеки НСД; відсутність реєстрації інцидентів і т.п.
Уразливості інформаційної мережі критичного застосування
- *Конфігурація мережі:* невідповідність архітектури мережевої безпеки; відсутність контролю потоку даних; неякісно налаштовані параметри безпеки обладнання; відсутність резервування конфігурації мережевого пристрою; передача паролів у незахищеному вигляді; недостатньо часта зміна паролів доступу до мережевих пристроїв; неадекватність контролю доступу до мережевих пристроїв; недостатній рівень фізичного захисту мережевого обладнання; НСД до портів мережевого обладнання; - *Периметр мережі:* не визначений периметр безпеки; відсутній або неправильно налаштований між мережевий екран; мережі управління використовуються для трафіку інших типів; управління мережевими сервісами інформаційної мережі критичного застосування реалізується в мережі ІТ; - *Моніторинг мережі:* неадекватні журнали між мережевого екрану; відсутність регулярного моніторингу безпеки в мережі; - *З'єднання:* не ідентифікуються критичні шляхи контролю та управління; використання стандартних протоколів зв'язку; відсутня або недостатня аутентифікація користувачів, даних або пристроїв; відсутність перевірки цілісності з'єднань; - *Бездротові мережі:* невідповідність аутентифікації між бездротовими клієнтами і точками доступу; невідповідний захист даних між бездротовими клієнтами і точками доступу.

Рис. 3. Основні зовнішні і внутрішні фактори, які впливають на захист інформації в системах критичного застосування

Ймовірність другої події розраховується за формулою $p_2 = N_{розр} / N_{заг}$, де $N_{розр}, N_{заг}$ – кількість розглянутих та загальна кількість можливих варіантів СЗІ. У разі використання методу повного перебору $p_2 = 1$.

Оцінку p_3 розглянемо наступним чином. Нехай за результатами застосування n методів багато вимірювального порівняльного аналізу отримана множина варіантів, причому i-й метод розпізнає найкращий варіант з ймовірністю p_i. За результатами застосування n методів j-й варіант за k методами був визначений як найкращий, а $n-k$ методів його найкращим не визнали. Необхідно оцінити достовірність того, що j-й варіант дійсно є найкращим. Достовірність класифікації j-го варіанту як найкращого оцінюється через перевищення порогу похибки класифікації d:

$$\frac{k\prod_{i=1}^{k} p_i + (n-k)\prod_{i=1}^{n-k}(1-p_i)}{k\prod_{i=1}^{k}(1-p_i) + (n-k)\prod_{i=1}^{n-k} p_i} \succ d. \qquad (1)$$

Таблиця 2.

Оцінювання ймовірності першої події за вербальними оцінками експерта

Вербальна оцінка впевненості експерта в адекватності варіанту СЗІ	Ймовірнісний еквівалент
Дуже незначна	0.01-0.1
Незначна	0.1-0.2
Помірна	0.2-0.4
Середня	0.4-0.6
Суттєва	0.6-0.8
Значна	0.8-0.9
Дуже велика	0.9-0.99

Якщо після оцінювання за (1) множина варіантів не пуста, тоді ймовірність наявності у цій множині найкращих варіантів визначається як:

$$p_m = 1 - \left\{1 - \prod_{j=1}^{m}\left[\frac{k_j}{n}\prod_{i=1}^{k_j} p_i + \frac{n-k_j}{n}\prod_{i=1}^{n-k_j}(1-p_i)\right]\right\}. \qquad (2)$$

При цьому вважається, що результати, отримані за різними методами багато вимірювального порівняльного аналізу, є збіжними.

Якщо ж консультації з експертами не проводилися та їх погляди на зміст поняття «раціональний» (оптимальний) варіант невідомі, значення p_3 може бути оцінено як:

$$p_3 = \frac{N_{важ}^{вик} N_{перетв}^{вик} N_{метод}^{вик}}{N_{важ} N_{перетв} N_{метод}}, \qquad (3)$$

де $N_{важ}^{вик}$, $N_{важ}$ – кількість використаних та можливих варіантів урахування важливості показників відповідно; $N_{перетв}^{вик}$, $N_{перетв}$ – кількість використаних та можливих варіантів переходу від реальних значень показників до розрахункових відповідно; $N_{метод}^{вик}$, $N_{метод}$ – кількість використаних та можливих методів порівняння альтернатив відповідно.

Висновки та напрямки подальших досліджень

Встановлена залежність ефективності захисту інформації СЗІ, які проектуються для ОКІ, що ґрунтуються на комплексному використанні методів групового врахування аргументів, аналогій, експертного оцінювання та статистичного оброблення даних. Зазначена залежність покладена в основу підходу до обґрунтування основних загальносистемних вимог до СЗІ. Застосування такого підходу розширює можливості аналізу в предметній області процесів управління складних систем. Напрямком подальших досліджень слід вважати подальше удосконалення та використання наведеного підходу під час удосконалення методичної бази щодо обґрунтування

проектуємих СЗІ та створення (переробки) відповідних нормативно-правових та керівних документів у сфері технічного захисту інформації.

Список літератури

1. Павлов, І.М. Формалізація проектних показників якості захисту інформації комплексної системи захисту інформації [Текст] / І.М. Павлов, В.О. Бірюков. // Захист інформації. – Київ: 2011. – № 2(51). – С. 15 – 21.
2. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [Текст] / НД ТЗІ 3.7 – 003 – 05. – К.: 2005. – 35 с.
3. Малюк, А.А. Информационная безопасность: Концептуальные и методологические основы защиты информации / А.А. Малюк. – М.: Высшая школа, 2004. – 280 с.
4. Широчин, В.П. Вопросы проектирования средств защиты информации в компьютерных системах и сетях / В.П. Широчин, В.Е. Мухин. – К.: 2000. – 111 с.
5. Щеглов, А.Ю. Проблемы и принципы проектирования систем защиты информации от НСД [Текст] / А.Ю. Щеглов. // Сборник "Экономика и производство". – М.: 2001. – № 3. – С. 34 – 46.
6. Проект Закону України "Про внесення змін до деякий законів України щодо забезпечення кібернетичної безпеки України" (зареєстрований № 11125 від 31.01.12).
7. Гончар, С.Ф. Проблеми забезпечення інформаційної безпеки критичної інфраструктури держави: актуальність, особливості, вразливості, загрози, завдання / С.Ф. Гончар, О.В. Коваль. // Збірник наукових праць ЦНДІ ЗСУ. Київ: 2013. – № 4 (66). – С. 280 – 291.
8. Потьомкін, М.М. Загальний підхід до формування вимог до складних систем [Текст] / М.М. Потьомкін, А.А. Седляр // Збірник наукових праць ЦНДІ ЗСУ. Київ: 2013. – № 3 (65). – С. 267 – 281.
9. Кобозева, А.А. Анализ информационной безопасности / А.А. Кобозева, В.А. Хорошко. – К.: изд. ГУИКТ, 2009. – 251 с.
10. Павлов, І.М. Проектування комплексних систем захисту інформації / І.М. Павлов, В.О. Хорошко. – К.: вид. ДУІКТ, 2011. – 245 с.
11. Загорка, О.М. Елементи дослідження складних систем військового призначення [Текст] / О.М. Загорка, С.П. Масов, А.І. Сбітнєв, П.І. Стужук. – К.: НАОУ, 2005. – 100 с.
12. Waldrop, M. Toward a Unified Theory of Cognition [Text] / M. Waldrop. – Science. – 1988. – Vol. 241. – № 27. – P. 27 – 29.

МЕТОДОЛОГИЯ ОБОСНОВАНИЯ ОСНОВНЫХ ОБЩЕСИСТЕМНЫХ ТРЕБОВАНИЙ К ПРОЕКТИРОВАНИЮ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЬЕКТАХ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

И.Н. Павлов

Государственный университет телекоммуникаций,
ул. Соломенская, 7, Киев, 03680, Украина; e-mail: pavlov@ukr.net

В статье предлагаются методики в составе методологии обоснования основных общесистемных требований к проектированию систем защиты информации на основе методов группового учёта аргументов, аналогий, экспертной оценки и статистической обработки данных.

Ключевые слова: методология, методики, свойства, система защиты информации, требования.

STRATEGY FOR JUSTIFICATION OF BASIC GENERAL SYSTEM REQUIREMENTS FOR DESIGNING DATA SECURITY SYSTEMS FOR CRITICAL INFRASTRUCTURES

I.N. Pavlov

State University of Telecommunications,
7, Solomenskaya Str., Kyiv, 03680, Ukraine; e-mail: pavlov@ukr.net

In this paper, the authors propose the techniques incorporated into a strategy for justification of basic general system requirements for designing data security systems based on group argument accounting methods, analogy approach, expert assessment methods, and statistical data processing methods.

Keywords: strategy, techniques, features, data security systems, requirements.