УДК 004.056.53

Бурячок В.Л.
Державний університет телекомунікацій
Грищук Р. В.
Житомирський військовий інститут імені С. П. Корольова Державного університету телекомунікацій
Мамарєв В. М.
Національний центр управління та випробувань космічних засобів

НАУКОВО-ТЕХНІЧНЕ ОБҐРУНТУВАННЯ ВИБОРУ ПІДХОДУ ДО ФОРМУВАННЯ МНОЖИНИ ІНФОРМАТИВНИХ ПАРАМЕТРІВ ДЛЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Анотація:
Вперше на основі методу скалярних згорток проведено науково-технічне обґрунтування вибору підходу до формування множини інформативних параметрів для систем захисту інформації. Одержано кількісні та якісні оцінки ефективності, що забезпечують науково обґрунтований вибір одного або декількох з досліджуваних підходів.

Постановка проблеми. Однією із основних задач системи інформаційної безпеки на етапі експлуатації інформаційно-телекомунікаційної системи є забезпечення нею заданих показників захищеності [1]. Складовою частиною системи інформаційної безпеки на яку безпосередньо покладається дана функція є система захисту інформації (СЗІ), що забезпечує розпізнавання легітимності виконання операцій з інформацією шляхом віднесення суб'єкта до певної категорії за встановленими правами. Класифікація таких суб'єктів СЗІ виконується на основі аналізу множини заздалегідь обраних параметрів, що називаються інформативними, а їх множина – множиною інформативних параметрів.

Відомо, що нині основним способом формування множин інформативних параметрів для СЗІ є евристичний підхід [2, 3]. Але одними з головних його недоліків при цьому залишаються неформалізовані й в більшості випадків суб'єктивні процедури відбору інформативних параметрів. Тому на сьогодні задача щодо обґрунтування науково обґрунтованого підходу до формування множини інформативних параметрів для СЗІ й досі залишається актуальною та потребує свого розв'язання.

Аналіз останніх досліджень і публікацій [4–7] показав, що окрім евристичного підходу до формування множини інформативних параметрів для СЗІ як альтернативний може бути використаний статистичний підхід. Згідно зі статистичним підходом, у разі статистичної незалежності інформативних параметрів, формування відповідної множини зводиться до оцінювання інформативності як суми інформативностей окремих параметрів [4]. Але з результатів експериментальних досліджень [5, 6] встановлено, що інформативні параметри є статистично залежними, що суттєво обмежує область застосування статистичного підходу. Ґрунтовний аналіз інших відомих підходів до оцінювання інформативності множини параметрів розкрито в [7], де показано що вибір того чи іншого параметру повинен спиратися на один або кілька критеріїв. Вибір таких критеріїв, як правило, також пов'язаний з рядом суб'єктивних процедур, а самі підходи потребують адаптації до тих завдань, які покладаються на конкретну СЗІ.

Метою статті є науково-технічне обґрунтування вибору підходу до формування множини інформативних параметрів для СЗІ.

Основні матеріали дослідження. З практики експлуатації СЗІ в інформаційно-комунікаційних системах встановлено, що такі системи захисту, як системи виявлення

атак, ґрунтуються на двох засадницьких принципах – виявлення аномалій та виявлення зловживань [1, 2]. В обох випадках вхідними даними для роботи системи виступають сформовані на основі множини інформативних параметрів шаблони поведінки – паттерни подій. Задача виявлення атаки за такої постановки зводиться до розпізнавання шаблону поведінки системи і фіксації факту її початку. Але як і в першому, так і в другому випадках множина інформативних параметрів підлягає оцінюванню на перемет її інформативності.

Систематизувавши відомі підходи до оцінювання інформативності параметрів, подамо їх у вигляді схеми (рис. 1).

Рис. 1. Структуризація базових підходів до оцінювання інформативності параметрів

Процедура вибору одного з наведених вище підходів (див. рис. 1) та адаптація його до формування множини інформативних параметрів для СЗІ повинна спиратися на один або кілька критеріїв якості.

Для порівняння відомих підходів між собою оберемо такі критерії якості: ступінь математичного обґрунтування підходу (Крит. 1); відносна складність реалізації підходу (Крит. 2); відносна швидкість процедур оцінювання інформативності параметрів (Крит. 3); якість параметрів, інформативність яких підлягає оцінюванню (Крит. 4). Спираючись на лінгвістичні оцінки приведені в [7] за визначеними вище критеріями, подамо їх у вигляді стовпчастої діаграми (рис. 2).

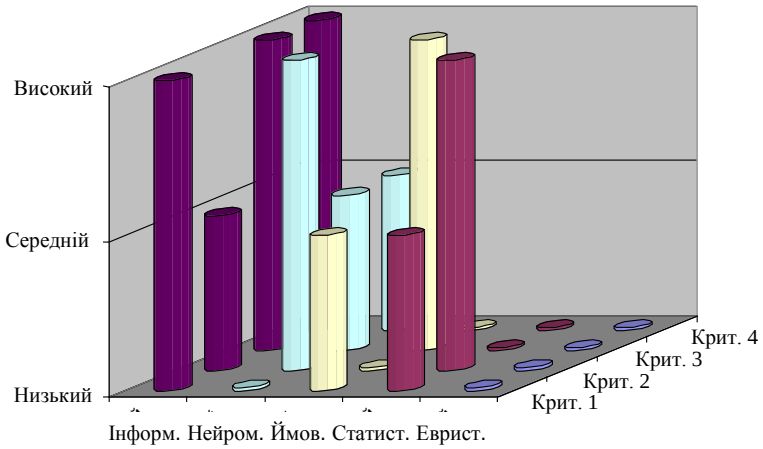

Рис. 2. Діаграма розподілу критеріїв якості залежно від обраного підходу до оцінювання інформативності параметрів

Поданий на рис. 2 якісний аналіз порівняння відомих підходів оцінювання інформативності параметрів не забезпечує в повній мірі обґрунтований вибір одного з них для вирішення поставленого завдання. Тому для науково-технічного обґрунтування вибору одного з відомих підходів (див. рис. 1) до формування множини інформативних параметрів, скористаємося аналітичною процедурою, яку реалізує метод вкладених скалярних згорток [8].

Нехай скалярна згортка y^* частинних критеріїв y^j на j - му рівні ієрархії, що мають відповідний пріоритет p^j, виступатиме оцінкою ефективності обраного підходу. Тоді алгоритм розв'язку задачі методом вкладених скалярних згорток може бути поданий ітераційною послідовністю операцій зваженої скалярної згортки векторних критеріїв з урахуванням векторів пріоритету на основі обраної схеми компромісів, тобто

$$y^{j-1}, p^{j-1} \to y^j \Big|_{j \in 2,m}. \quad (1)$$

Спираючись на алгоритм (1) оцінку ефективності підходу до формування множини інформативних параметрів для СЗІ формалізуємо як задачу з визначення скалярної згортки критеріїв

$$y^* = y^m. \quad (2)$$

Згідно з [8] для методу вкладених скалярних згорток (1) як схему компромісів доцільно обрати нелінійну схему, оскільки науковим підґрунтям для її використання є те, що вона, на відміну від відомих, передбачає мінімізацію усіх частинних критеріїв які входять до її складу за відповідних обмежень на кожен з них, тобто

$$0 \le y_i^j \le A_i^j, \; A = A_i \Big|_{i \in 1,n}^{j \in 1,m},$$

де A – вектор обмежень;

j – рівень ієрархії частинного критерію, $j \in 1,m$;

i – кількість частинних критеріїв на j - му рівні ієрархії, $i \in 1,n$.

Таким чином, з урахуванням описаного вище алгоритму (1) задача з оцінювання ефективності підходу до формування множини інформативних параметрів для СЗІ (2), набуватиме вигляду

$$y_0^* = 1 - \frac{1}{\sum_{i=1}^{n_1} p_{i1}^{(1)} (1 - y_{i1}^{(1)})^{-1}}. \quad (3)$$

Для застосування на практиці запропонованого підходу подамо обрані вище частинні критерії у вигляді однорівневої ієрархічної схеми (рис. 3).

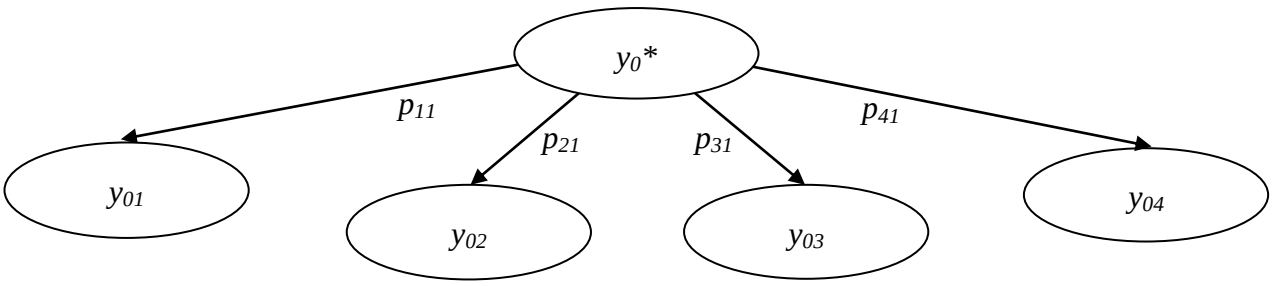

Рис. 3. Схема однорівневої ієрархії частинних критеріїв

Відповідно до структурної схеми (див. рис. 3) y_{01}, y_{02}, y_{03}, y_{04} – це числові значення частинних критеріїв, а p_{11}, p_{21} p_{31}, p_{41} – це відповідні їм коефіцієнти пріоритету.

Припустимо, що усі частинні критерії є рівноважливими, тобто $p_{11} = p_{21} = \ldots = p_{41}$. Якщо виходити з того, що вага критеріїв повинна задовольняти умові $\sum_{i=1}^{n} p_{i1} = 1$, де $n = 4$, то пріоритет кожного з критеріїв визначатиметься як $p_{i1} = 0.25$.

Скориставшись методикою [8, 9] в табл. 1 подамо кількісні значення частинних критеріїв для досліджуваних підходів.

Таблиця 1.

Вихідні дані для оцінювання ефективності досліджуваних підходів

Підходи	Критерій оцінювання			
	y_{01}	y_{02}	y_{03}	y_{04}
Інформаційний	0.17	0.33	0.17	0.17
Нейромережевий	0.5	0.17	0.33	0.33
Ймовірнісний	0.33	0.5	0.17	0.5
Статистичний	0.33	0.17	0.5	0.5
Евристичний	0.5	0.5	0.5	0.5

Скориставшись розробленим підходом (1)–(3), та спираючись на дані табл. 1, маємо: для інформаційного підходу

$$y_0^* = 1 - \frac{1}{0.25\frac{1}{1-0.17} + 0.25\frac{1}{1-0.33} + 0.25\frac{1}{1-0.17} + 0.25\frac{1}{1-0.17}} = 0.22;$$

для нейромережевого підходу

$$y_0^* = 1 - \frac{1}{0.25\frac{1}{1-0.5} + 0.25\frac{1}{1-0.17} + 0.25\frac{1}{1-0.33} + 0.25\frac{1}{1-0.33}} = 0.36;$$

для ймовірнісного підходу

$$y_0^* = 1 - \frac{1}{0.25\frac{1}{1-0.33} + 0.25\frac{1}{1-0.5} + 0.25\frac{1}{1-0.17} + 0.25\frac{1}{1-0.5}} = 0.4;$$

для статистичного підходу

$$y_0^* = 1 - \frac{1}{0.25\frac{1}{1-0.33} + 0.25\frac{1}{1-0.17} + 0.25\frac{1}{1-0.5} + 0.25\frac{1}{1-0.5}} = 0.4;$$

для евристичного підходу

$$y_0^* = 1 - \frac{1}{0.25\frac{1}{1-0.5} + 0.25\frac{1}{1-0.5} + 0.25\frac{1}{1-0.5} + 0.25\frac{1}{1-0.5}} = 0.5.$$

Співставивши одержані кількісні оцінки з якісною лінгвістичною фундаментальною оберненою шкалою, подамо результати порівняння ефективності досліджуваних підходів у вигляді узагальненої табл. 2.

Таблиця 2.

Узагальнені дані за результатами оцінювання ефективності досліджуваних підходів

Підходи	Оцінка ефективності	
	кількісна	якісна
Інформаційний	0.22	достатня
Нейромережевий	0.36	достатня
Ймовірнісний	0.4	задовільна
Статистичний	0.4	задовільна
Евристичний	0.5	низька

Аналіз одержаних результатів (див. табл. 2) дозволяє зробити висновок: інформаційний підхід за усіх рівних початкових умов є найефективнішим серед досліджених підходів й може бути застосований для формування множини інформативних параметрів для систем захисту інформації. Як альтернативний інформаційному, але такий, що має гірші показники ефективності може бути використаний нейромережевий підхід, який забезпечує достатньо якісне формування множини інформативних параметрів. Решта досліджених підходів не в змозі забезпечити ефективне вирішення поставленої задачі.

Висновки і перспективи подальшої роботи. Вперше на основі методу скалярних згорток проведено науково-технічне обґрунтування вибору підходу до формування множини інформативних параметрів для систем захисту інформації. Як результат, одержано кількісні та якісні оцінки ефективності, що забезпечують науково обґрунтований вибір одного або декількох з досліджуваних підходів.

У результаті дослідження встановлено, що для формування множини інформативних параметрів для систем захисту інформації найдоцільніше використовувати інформаційний підхід.

Подальші дослідженні будуть спрямовані на автоматизацію процесу формування множини інформативних параметрів для систем захисту інформації на основі інформативного підходу.

Список використаних джерел:

1. *Ленков С. В. Методы и средства защиты информации : монография [в 2-х т.] Т. 2. Информационная безопасность / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. – К. : Арий, 2008. – 344 с.*

2. *Лукацкий А.В. Обнаружение атак / Лукацкий Алексей Викторович. – СПб : БХВ-Петербург, 2001. – 624 с.*

3. *D. Opitz «Popular ensemble methods: An empirical study» / D. Opitz, R. Maclin // Journal of Artificial Intelligence Research, 1999. – №11. – P. 169–198.*

4. *Айвазян С. А. Прикладная статистика. Классификация и снижение размерности / С. А. Айвазян, В. М. Бухштабер, И. С. Ешоков [та ін]. – М. : ФиС, 1989. – 607 с.*

5. *Дуда Р. Распознавания образов и анализ сцен / Р. Дуда, П. Харт. – М. : Мир, 1976. – 512 с.*

6. *Вентцель Е.С. Исследование операций / Вентцель Елена Сергеевна. – М. : «Наука», 1980. – 208 с.*

7. Дубровин В. И. Интеллектуальные средства диагностики прогнозирования надежности авиадвигателей / В.И. Дубровин, С.А. Субботин, А.В. Богуслаев, В.К. Яценко : [монография]. – Запорожье : ОАО «Мотор-Сич», 2003.– 279 с.

8. Воронин А. Н. Многокритериальные решения: модели и методы : монография / А. Н. Воронин, Ю. К. Зиатдинов, М. В. Куклинский. – К. : НАУ, 2011. – 348 с.

9. Паклин Н. Б. Бизнес-аналитика. От данных к знаниям. 2-е изд. / Н. Б. Паклин, В. И. Орешков. – СПб. : Питер, 2010. – 704 с.