УДК 004.45

Гладиш С. В., Кононович В. Г.
Gladysh S. V., Kononovich V. G.

РЕАГУВАННЯ ТА ОБРОБКА ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МУЛЬТИАГЕНТНОЮ СИСТЕМОЮ

INFORMATION SECURITY INCIDENTS RESPONSE AND HANDLING BY A MULTIAGENT SYSTEM

Анотація. Запропоновано за допомогою мультиагентної системи реагувати та обробляти інциденти інформаційної безпеки. Визначено нові необхідні терміни. Запропоновано структуру та функції системи. Для формалізації вибору варіантів розподілу ресурсів використано нечіткі множини.

Summary. The processes of information security incident response and handling is proposed to realize by a multi-agent system. New necessary terms are defined. The structure and functions of the system are developed. Fuzzy sets are used to formalize choosing variants of resources distribution.

Розподіленість сучасних інформаційних середовищ та розпаралеленість процесів обробки інформації в них завдяки використанню мультиагентних систем (МС) [1, 2] несуть в собі як значні переваги, так і нові ризики та побічні негативні явища, зокрема *проблему інформаційної безпеки (ІБ)*, яка проявляється у виникненні *інцидентів ІБ* [3].

В роботах [1, 4, 5] використано технологію МС як метод дослідження та вирішення завдань ІБ: розроблено комплекс взаємопов'язаних ймовірнісних, автоматних моделей [1] та мережу Петрі [4], які дозволяють використовувати принципи штучної імунної системи [5]. Як приклад використання цих моделей розглянуто МС керування міжмереженими екранами [1]. Схожими за використанням технології МС та загальною вирішуваною проблемою ІБ, є декілька інших досліджень, зокрема [6, 7], які відрізняються рівнем формалізації завдання, математичним апаратом, метою та предметом досліджень.

Часткове вирішення завдань безпеки самих МС розпочато в [8 ... 11]. Вразливість комунікацій МС, якій присвячено дослідницький проект [8], *не є єдиним* фактором спричинення інцидентів ІБ. Дослідження [9] розглядає *здебільш* можливість атакування агентами цільової платформи та *лише окремі* аспекти безпеки самих агентів. В роботах [10, 11] розглянуто *тільки* забезпечення цілісності та конфіденційності коду агентів криптографічними методами.

Однак принаймні у відкритих наукових виданнях не ставилось завдання реагування та обробки інцидентів ІБ за допомогою МС. Причина – відсутність формалізованої моделі та алгоритму, які дозволяли б за принципом «керованого моделлю проектування» створити мультиагентну систему реагування та обробки інцидентів ІБ (МСРОІ).

Мета дослідження: розробити формалізований опис структури та функцій реагування та обробки інцидентів ІБ за допомогою МСРОІ.

Введемо нові визначення, які знадобляться під час дослідження:

Агентно-орієнтований набір ресурсів ІБ – множина ресурсів ІБ, які має МСРОІ.

Інцидентно-орієнтований набір ресурсів ІБ - підмножина ресурсів ІБ, якими розполагає МСРОІ, і які в сукупності є достатніми для реагування на конкретний тип інцидентів ІБ.

Тестовий набір ресурсів ІБ - підмножина ресурсів ІБ, які відбираються для попередньої імітації, прогнозу та адаптації до відомого або невідомого типу інциденту ІБ.

Набір атакуючих ресурсів інциденту ІБ – підмножина ресурсів, які використовуються для здійснення конкретного типу інциденту ІБ.

Процеси реагування та обробки інцидентів ІБ нерозривно поєднані з процесом виявлення вторгнень. Тому автори розглядатимуть МСРОІ у взаємодії з підсистемою виявлення вторгнень (IDS). Бо саме IDS видає початковий сигнал про інцидент ІБ, і з цього сигналу від IDS розпочинається подальше реагування та обробка.

Виходячи з цього, створимо функціональну та ієрархічну структуру МСРОІ (рис. 1).

Рисунок 1 - Функціональна схема мультиагентної системи реагування та обробки інцидентів

Розглянемо три функціональні класи агентів: агенти-детектори; агенти-координатори; агенти-реактори; та 6 ієрархічних рівнів підсистем у складі МСРОІ:
підсистема виявлення вторгнень (IDS); база знань ідентифікації інцидентів ІБ; підсистема реагування на інциденти ІБ; база знань реагування на інциденти ІБ; підсистема обробки інцидентів ІБ; підсистема зворотного зв'язку.

Виділимо наступні етапи реагування та обробки інцидентів ІБ за допомогою МСРОІ:

1) індикація агентами-детекторами будь-якої підозрілої активності;
2) ідентифікація IDS активності як певного типу інциденту ІБ за умови знаходження в базі знань сигнатури або виявлення аномалії по відношенню до еталону поведінки;
3) отримання підсистемою реагування сигналу від IDS про ідентифікований відомий або невідомий інцидент;
4) ідентифікація набора атакуючих ресурсів інциденту за наявності в базі знань кореляції між характеристиками сигналу про інцидент та записами про набори атакуючих ресурсів;
5) формування тестових наборів ресурсів ІБ за алгоритмом, що знаходиться в базі знань;
6) імітаційне моделювання ефективності перекриття тестовим набором ресурсів – ідентифікованого набору атакуючих ресурсів за моделлю, що знаходиться в базі знань;
7) прийняття рішення щодо вибору інцидентно-орієнтованого набору ресурсів ІБ;
8) видача підсистемою обробки керуючого сигналу агентам-реакторам щодо обробки інциденту за допомогою інцидентно-орієнтованого набору ресурсів ІБ;
9) оцінка підсистемою зворотного зв'язку та агентами-детекторами ефективності використання інцидентно-орієнтованого набору ресурсів ІБ, поповнення баз знань новим досвідом, аналіз інциденту та синтез керуючого сигналу щодо превентивних дій.

Переробимо загально-абстрактну класичну модель системи захисту інформації з повним перекриттям загроз [12] у відповідності до умов завдання реагування та обробки інцидентів ІБ за допомогою МСРОІ. Для цього будемо використовувати математичний апарат теорії множин [13]. Змінимо базовий кортеж, який тепер складатиметься з наступних множин $\langle C, X, R, A \rangle$, які ми доповнимо їх підмножинами:

$\{c\} \in C$ - множина типів інцидентів ІБ;

$\{x\} \in X$ - множина атакуючих ресурсів;

$\{r\} \in R$ - множина ресурсів ІБ;

$\{x_n\} \in X^c$ - набір атакуючих ресурсів окремого типу інциденту ІБ *c*;

$\{a_k\} \in A$ - множина агентів, що утворює МСРОІ;

$\{r_k\} \in R^A$ - агентно-орієнтований набір ресурсів ІБ, якими керує конкретна МСРОІ *A*;

$\{y_n\} \in Y^c$ – інцидентно-орієнтований набір ресурсів ІБ (підмножина ресурсів ІБ), які достатньо використати для ефективного реагування та обробки інциденту с.

Зробимо декілька припущень:

1) будь-який атакуючий ресурс може бути повністю нейтралізовано певним ресурсом ІБ:

$$\forall x_i \; \exists r_j \quad \wedge \quad x_i + r_j \geq 0; \tag{1}$$

2) множина ресурсів ІБ повністю перекриває множину атакуючих ресурсів:

$$ord\ R \geq ord\ X \quad \wedge \quad \sum\{r\} \geq \sum\{x\}; \tag{2}$$

3) набір атакуючих ресурсів будь-якого типу інциденту є комбінацією (підмножиною), утвореною з єлементів множини всіх атакуючих ресурсів:

$$X^c \subseteq X, \ \forall c; \tag{3}$$

4) будь-який агентно-орієнтований набір ресурсів ІБ є комбінацією (підмножиною), утвореною з єлементів множини всіх ресурсів ІБ:

$$R^A \subseteq R, \ \forall A; \tag{4}$$

5) будь-який набір атакуючих ресурсів певного типу інциденту може бути повністю перекритий агентно-орієнтованим набором ресурсів ІБ:

$$\forall c \ \exists \ A \quad \wedge \quad ord\ R^A \geq ord\ X^c \quad \wedge \quad \sum_{j=1\ldots k}^{k} \{r_j\} \geq \sum_{i=1\ldots n}^{n} \{x_i\}. \tag{5}$$

Елементи цих множин та їх підмножини можуть бути певним чином взаємопов′язані між собою певними відносинами, які для кожного конкретного випадку і опистують структуру МСРОІ. В результаті отримуємо чотиридольний граф (рис. 2), вершинами якого є елементи кортежу $\langle C, X, R, A \rangle$, а дугами – взаємозв'язки, що відображають процеси реагування та обробки інцидентів ІБ за допомогою МСРОІ.

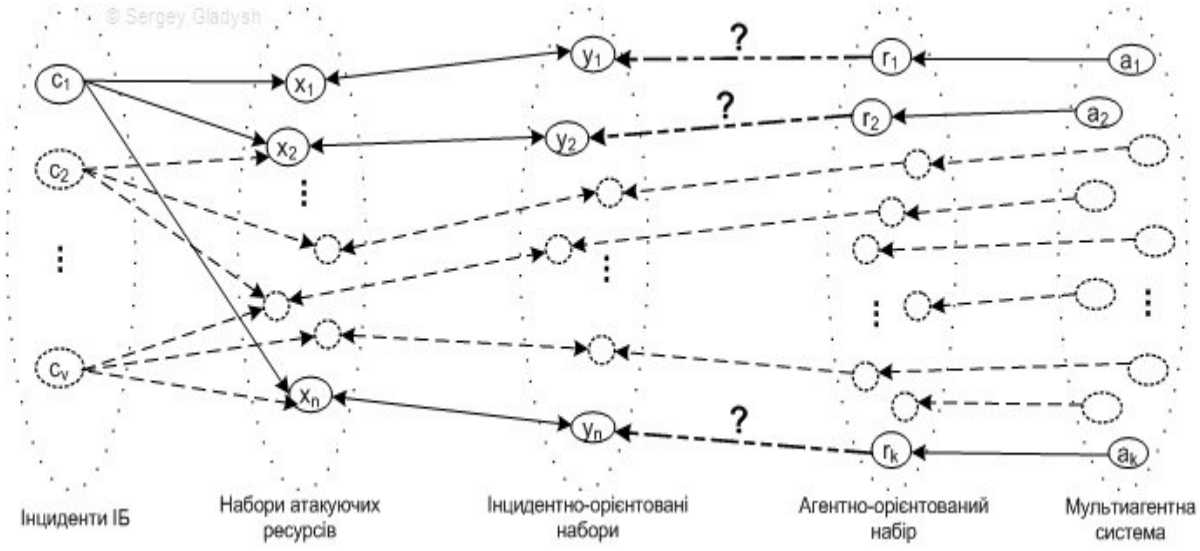

Рисунок 2 – Граф, що відображає структуру МСРОІ

Під час аналізу альтернатив виникає необхідність розрахунку, порівняння, розподілу ресурсів ІБ. Якщо в процесі прийняття рішень, оцінки та вибору альтернатив користуватись традиційними (чіткими) алгоритмами - в умовах невизначеності початкових даних та нечіткості постановки завдання буде вноситись додаткова некоректність, що збільшуватиме тим самим початкову невизначеність. Даний процес вимагає залучення адекватного математичного апарату для його опису. Процес прийняття рішення щодо того, як реагувати на інцидент ІБ представимо нечіткими множинами [14] та операцією відображення:

$$\widetilde{D}^c \left(X^c, A, R^A \right) \ : \ \{ r_k \} \in R^A \ \overset{\mu_{Yc}}{\rightarrow} \ \{ y_n \} \in Y^c , \tag{6}$$

де $\widetilde{D}^c$ – нечітка операція прийняття рішення МСРОІ щодо формування інцидентно-орієнтованого набору ресурсів ІБ;

$\mu_{Yc}(r_j)$ – функція належності ресурса $r_j \in R^A$ до інцидентно-орієнтованого набору Y^c.

Можемо конкретизувати вид функції належності елементів агентно-орієнтованого набору до інцидентно-орієнтованого набору. На даному етапі дослідження задамо її як трапецевидну функцію належності:

$$\mu_{Yc}(r_j) = \begin{cases} 0, & if \ r_j \le a_j; \\ \dfrac{(x_{ij} - a_{ij})}{(b_{ij} - a_{ij})}, & if \ a_j < r_j \le b_j; \\ 1, & if \ b_j < r_j \le c_j; \\ \dfrac{(d_{ij} - x_{ij})}{(d_{ij} - c_{ij})}, & if \ c_j < r_j \le d_j; \\ 0, & if \ d_j < r_j. \end{cases} \tag{7}$$

Такий вид функції належності надає можливості представляти лінгвістичні терми як нечіткі (L-R)-величини у вигляді трапецевидгних нечітких інтервалів $\langle a_j, b_j, c_j, d_j \rangle$, що дуже зручно з обчислювальної точки зору.

Вирішальне значення під час формального опису запропонованої процедури мають умови невизначеності факту формування певного інцидентно-орієнтованого $\{ y_n \} \in Y^c$ набору з елементів агентно-орієнтованого набору ресурсів ІБ $\{ r_k \} \in R^A$.

Початкові невизначеності станів (входження) елементів $r_j \in R^A$ множини агентно-орієнтованого набору ресурсів ІБ до інцидентно-орієнтованого набору $\{ y_n \} \in Y^c$, зумовлені непередбаченістю інцидентів ІБ, і можуть бути описані нечіткою множиною $\widetilde{Z}^{Yc}$:

$$\widetilde{Z}^{Yc} \left(R^A \right) = \{ \langle \mu_{Yc}(r_j), \ Y^c \rangle \} = \{ \ \mu_{Yc}(r_1) / Y^c ; \mu_{Yc}(r_2) / Y^c ; \ldots ; \mu_{Yc}(r_k) / Y^c \ \} . \tag{8}$$

Оскільки МСРОІ повинна «вміти» прогнозувати нові типи інцидентів та адаптуватись до них в режимі реального часу, доцільним буде включення в процедуру прийняття рішення щодо формування інцидентно-орієнтованого набору - етапу дослідної імітації роботи МСРОІ шляхом формування тестових наборів ресурсів ІБ $\{ q_m \} \in Q^c$:

$$\widetilde{D}^c \ : \ R^A \ \overset{\mu_{Qc}}{\rightarrow} \ Q^c \ \overset{\mu_{Yc}}{\rightarrow} \ Y^c , \tag{9}$$

де $\{ q_m \} \in Q^c$ – множина тестових наборів, що вибираються серед елементів $r_j \in R^A$ агентно-орієнтованого набору ресурсів ІБ для прогнозування та адаптації до інциденту с;

$\mu_{Qc}(r_j)$ – функція належності ресурсу r_j до тестового набору $\{ q_m \} \in Q^c$, вид якої можна конкретизувати трапецевидною формою аналогічно формулі (7).

Невизначеності включення елементів $r_j \in R^A$ до тестового набору $\{q_m\} \in Q^c$ (формування тестових маршрутів) можуть бути описані нечіткою множиною $\tilde{Z}^{Qc}$:

$$\tilde{Z}^{Qc}(R^A) = \{\langle \mu_{Qc}(r_j),\ Q^c \rangle\} = \{\ \mu_{Qc}(r_1)/Q^c;\ \mu_{Qc}(r_2)/Q^c;\ \ldots;\ \mu_{Qc}(r_j)/Q^c\ \}. \qquad (10)$$

Таким чином, процедура прийняття рішення щодо формування інцидентно-орієнтованого набору ресурсів ІБ $\{y_n\} \in Y^c$ включатиме етап імітації процесу реагування на інцидент ІБ набором тестових маршрутів $\{q_m\} \in Q^c$, відповідно до алгоритму в режимі реального часу, з урахуванням вимог розробника та ПІБ. Цей етап потрібен, щоб реалізовувати процес відпрацювання стійкої працездатності МСРОІ.

Операцію прийняття рішення $\tilde{D}^c$ доцільно розбити на 2 рівні (рис. 3):

$$\tilde{D}^c = \tilde{D}_1^c \cup \tilde{D}_2^c; \qquad \tilde{D}_1^c : R^A \xrightarrow{\mu_{Qc}} Q^c; \qquad \tilde{D}_2^c : R^A \xrightarrow{\mu_{Yc}} Y^c \qquad (11)$$

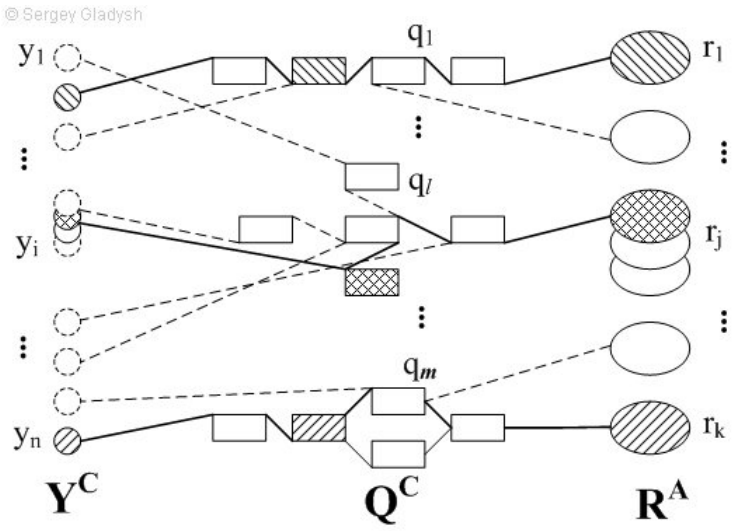

Рисунок 3 – Граф процесу формування тестових та інцидентно-орієнтованих наборів

Вважатимемо, що процес прийняття рішень, пов'язаних з формуванням інцидентно-орієнтованого набору ресурсів ІБ, реалізується шляхом виконання в режимі реального часу заданого комплексу взаємозв'язаних елементарних операцій так, щоб при заданих характеристиках ресурсів ІБ та типу інциденту ІБ оптимізувати вибрану цільову функцію, що виражає міру ефективності реагування на інцидент ІБ.

Таким чином, алгоритм формування кожного елемента (окремого ресурсу y_i) інцидентно-орієнтованого набору Y^c базуватиметься на обробці результатів оцінки працездатності окремих елементів при імітації процесу реагування на інцидент ІБ окремим маршрутом $q_l \in Q^c$.

Отже, процеси реагування та обробки інциденту ІБ за допомогою МСРОІ можемо описати кортежем:

$$\tilde{\Psi} = \langle C, X^c, A, R^A, \tilde{D}_1^c, \tilde{D}_2^c, \tilde{Z}^{Qc}, \tilde{Z}^{Yc}, Q^c, Y^c \rangle, \qquad (12)$$

де $\tilde{\Psi}$ - нечітка модель (функціонал), що виражає відповідності:

$$q_l = \tilde{\Psi}\ (X^A, R^c, \tilde{D}_1^c, \tilde{Z}^{Qc}), \qquad y_i = \tilde{\Psi}\ (X^A, R^c, Q^c, \tilde{D}_2^c, \tilde{Z}^{Yc}). \qquad (13)$$

Підводячи підсумок, відмітимо, що завдання реагування та обробки інцидентів ІБ вирішено за допомогою МСРОІ. Було визначено нові термін, розроблено модель та зроблено припущення, які обмежили простір пошуку вимогами конкретного вирішуваного завдання. Розроблено структуру та функції МСРОІ, процеси функціонування якої формалізовано за допомогою математичного апарату

теорії нечітких множин. Отримані результати можуть бути використані під час проектування систем реагування та обробки інцидентів ІБ.

Література

1. *Кононович В.Г., Гладиш С.В.* Модель мультиагентної системи інформаційної безпеки в телекомунікаційній мережі // Наукові праці ОНАЗ ім. О.С.Попова. – 2007. - № 1. – С. 45-50.
2. *Martin D.L., Cheyer A.J., Moran D.B.* The Open Agent Architecture: A Framework for Building Distributed Software Systems. – New York: SRI International, 1998. – 242 p.
3. *Гладиш С.В., Кононович В.Г., Тардаскін М.Ф.* Порівняльний аналіз стандартів ISO/IEC та української нормативної бази в частині керування інцидентами інформаційної безпеки // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2007. – № 15.
4. *Гладиш С.В.* Ймовірнісна Petri-net модель взаємодії агента безпеки з телекомунікаційною мережею // Радиоэлектроника и молодежь в XXI веке: XI Международный молодежный форум, 10 – 12 апреля 2007 г. – Харьков: ХНУРЭ, 2007. – С. 123.
5. *Gladysh S.* A multi-agent immune approach to information security assurance in telecommunications // «Світ інформації та телекомунікацій - 2007»: IV міжнародна науково-технічна конференція, 12 – 13 квітня 2007 р. – К.: ДУІКТ, 2007. – с. 113.
6. *Kotenko I.* Agent-Based Modeling and Simulation of Cyber-Warfare between Malefactors and Security Agents in Internet // Simulation in wider Europe. ESM'05: 19th European Simulation Conference. – Berlin, 2005. – P. 78 – 90.
7. *Gorodetsky V., Karsaev O., Samoilov V., Ulanov A.* Asynchronous alert correlation in multi-agent intrusion detection systems // Lecture Notes in Computer Science, Vol.3685. - 2005.
8. *Valeyev S.S., Bakirov T.K., Pogorelov D.N.. Starodumov I.V.* Multiagent Technology and Information System Security // Proceedings of the 7th International Workshop on Computer Science and Information Technologies CSIT'2005. – Vol.1, Ufa, Russia, 2005. – P. 195-200.
9. *Szczypiorski K., Margasiński I., Mazurczyk W.* Trusted Communication Platform for Multi-Agent Systems: Research Project / European Research Office of US Army. - 2007. – 90 p.
10. *Page J., Zaslavsky A., Indrawan M.* Countering Agent Security Vulnerabilities using an Extended SENSE Schema // Proceedings of the IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT'04). - IEEE, 2004. – P. 166 – 180.
11. *Page J., Zaslavsky A., Indrawan M.* Countering Security Vulnerabilities in Agent Execution using a Self Executing Security Examination // Proceedings of the AAMAS'04. - ACM, 2004. – P. 44 – 51.
12. *Ameiller J., Robles S., Ortega-Ruiz J.A.* Self-Protected Mobile Agents // Proc. AAMAS'04. - ACM, 2004.
13. *Hoffman L.J.* Modern methods for computer security and privacy. - New Jersey: Prentice-Hall, Inc., Englewood Cliffs, 1977. – 264 p.
14. *Мелихов А.Н., Бернштейн Л.С.* Конечные чёткие и расплывчатые множества. – Таганрог, ТРТИ, 1981. – 146 с.
15. *Zadeh L.* Fuzzy sets // Information and Control. - 1965. – №8. - P. 338 – 353.