УДК 621.34

С.Г. Семенов, М.Й. Заполовський, О.І. Баленко

Національний технічний університет «ХПІ», Харків

КОМПЛЕКС МЕТОДІВ АДАПТИВНОГО УПРАВЛІННЯ БЕЗПЕКОЮ КОМП'ЮТЕРИЗОВАНИХ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ УПРАВЛЯЮЧИХ СИСТЕМ КРИТИЧНОГО ЗАСТОСУВАННЯ

У статті розроблено модель адаптивного управління безпекою комп'ютеризованих інформаційно-вимірювальних управляючих систем критичного застосування (КІВУСКЗ). Проведено дослідження та розроблено алгоритм виконання процедур управління безпекою КІВУСКЗ. На основі результатів дослідження запропоновано комплекс методів адаптивного управління безпекою КІВУСКЗ, що включає до себе адаптивний метод виявлення зловмисних зовнішніх впливів на КІВУСКЗ на основі нейронних мереж та метод синтезу нейронних мереж для виявлення шкідливого програмного забезпечення. Проведено дослідження та отримані результати тестування системи в умовах зловмисних впливів комп'ютерних атак.

Ключові слова: *комп'ютеризована інформаційно-вимірювальна управляюча система критичного застосування, комп'ютерні атаки, нейронні мережі, нейромережевий імунний детектор.*

Вступ

Активне впровадження комп'ютерних технологій критичного застосування в ключові сфери життєдіяльності суспільства є характерною рисою існування сучасної держави. Проте чим складніше завдання автоматизації і чим відповідальніше галузь, в якій використовуються комп'ютерні інформаційні технології, тим критичніше і жорсткіше стають вимоги до ключових показників, що визначають безпеку функціонування системи. Пов'язано це багато в чому з тим, що масове поширення комп'ютерних мережевих технологій істотно розширило можливості зловмисників у використанні методів і засобів несанкціонованого доступу до інформації. В той же час рівень розвитку засобів діагностування і реагування на деструктивні зміни режимів функціонування і внутрішніх характеристик КІВУСКЗ залишається колишнім.

Аналіз літератури [1 – 6] показав, що в теперішній час існує багато моделей та методів захисту інформації, але традиційні підходи забезпечення безпеки КІВУСКЗ спрямовані на виявлення аномальної поведінки елементів системи і ставлять метою усунення виявлених негативних симптомів у поведінці шляхом впливу на окремі вимірювані показники. Однак, при цьому причини відхилень у стані системи не виявляються. У ряді практичних випадків це призводить до аномальної зміни інших, неврахованих показників, виходу системи зі свого нормального стану, і як наслідок, зниження її ефективності.

1. Модель адаптивного управління безпекою КІВУСКЗ

Проведені дослідження [2, 4, 5] показали, що в теперішній час при вирішенні завдань управління безпекою взаємопов'язаних систем переважають підходи, в яких розглядаються тільки власно керовані підсистеми і системи не вимірюваних збурень. Однак на практиці КІВУСКЗ являють собою складні багатокомпонентні системи, що складаються з безлічі підсистем $S=\{S_1,S_2,\ldots,S_n\}$, кожна з яких має керуючі входи і відповідні цільові функціонали $U=\{u^{(1)},u^{(2)},\ldots,u^{(n)}\}$ – керуючі входи.

Для математично формалізованої постановки задачі адаптивного управління КІВУСКЗ в умовах зовнішніх впливів скористаємося такими положеннями [2]. Управління деякого об'єкта здійснюється в просторі станів об'єкта з використанням макрозмінних $\psi_i:\Re^{(k)}\to\Re,\ \psi_i\in C^1,\ i=1,\ldots,r,\ r\le k$, рівність нулю яких задає «бажані інваріантні різноманіття». Сам термін "інваріантні різноманіття" в роботі [2] вводиться через визначення фазового потоку $x(t,x_0,t_0)$, як відображення початкового стану $x_0\in\Re^{(k)},\ t_o,\ t\in\Re_+$ в стан *x(t)* в момент часу t, де $\Re$ – поле дійсних чисел, $\Re_+=\{x\in\Re|x\ge 0\}$, $\Re^{(k)}$ – лінійний простір $L(\Re)$ над полем дійсних чисел з розмірністю $\dim\{L(\Re)\}=k$.

Слід зазначити, що множини $S\subset\Re^{(k)}$, які характеризують структурно-функціональну побудову КІВУСКЗ, називаються інваріантними по відношенню до потоку станів характеристик $x(t,x_0,t_0)$, якщо $x(t,x_0,t_0)\in S$ для будь-яких $x_0\in S$ для всіх $t>t_0$.

Виходячи з цього, введемо термін «нормальні стани КІВУСКЗ», під яким будемо розуміти початкові стани системи, які задовольняють технічну мету забезпечення гарантованого рівня безпеки і одночасно є найбільш природними станами самого об'єкта.

В якості критерію безпеки КІВУСКЗ пропонується використовувати властивість аттрактивності

різноманіття станів системи. При цьому повинні виконуватися наступні властивості:

– різноманіття станів КІВУСКЗ має бути інваріантним до зовнішніх впливів;

– для деякої околиці V аттрактивної множини станів КІВУСКЗ D і для всіх $x_0 \in V$ виконуються наступні граничні співвідношення:

$$x(t, x_0) \in V \; \forall \; t \geq 0 ; \qquad (1)$$

$$\lim_{t \to \infty} \left\| x(t, x_0) \right\|_D = 0 . \qquad (2)$$

Розглянемо узагальнену структуру КІВУСКЗ в якій функції розподілу доступу і захисту інформації (управління безпекою) розосереджені між елементами системи. Нехай функції

$\psi_1 : \Re^{n_1} \times \Re_+ \to \Re, \psi_2 : \Re^{n_2} \times \Re_+ \to \Re, \ldots, \psi_n : \Re^{n_n} \times \Re_+ \to \Re$

задають цільові обмеження для систем $S_1, S_2, \ldots, S_n$ відповідно. Іншими словами, для деяких $u_1 \in \Re_+, u_2 \in \Re_+, \ldots, u_n \in \Re_+$ і моменту часу $t^* \in \Re_+$, нерівності

$$\left\| \psi_1(x(t), t) \right\|_{\infty, \left[t^*, \infty \right]} \leq u_1, \left\| \psi_2(y(t), t) \right\|_{\infty, \left[t^*, \infty \right]} \leq \leq u_2, \ldots, \left\| \psi_n(y(t), t) \right\|_{\infty, \left[t^*, \infty \right]} \leq u_n , \qquad (3)$$

визначають бажаний стан з'єднань елементів КІВУСКЗ (рис. 1). Метою синтезу адаптивного управління безпекою КІВУСКЗ є визначення функцій $u_1(x_1, t), u_2(x_2, t), \ldots, u_n(x_n, t)$ які забезпечують вирішення задач 1, 2.

Відмінною особливістю запропонованого підходу управління безпекою КІВУСКЗ є включення інформації про природні (або бажані) динамічні стани системи безпосередньо в цільову функцію.

Рис. 1. Алгоритм виконання процедур управління безпекою КІВУСКЗ

Проведені дослідження показали, що в даний час відомі методи і способи синтезу керування комп'ютерними системами. Однак, дуже часто ці рішення спрямовані на побудову загальних математичних моделей технічних систем і функціональних процесів, які відбуваються в них. При цьому нехтуються питання інформаційної безпеки. У разі використання КІВУСКЗ дана зневага неприпустима.

Для ефективного функціонування системи, та з метою синтезу адаптивного управління безпекою КІВУСКЗ пропонується використовувати підхід, основний на оцінці аттрактивного стану системи з урахуванням її чутливості до зовнішніх впливів.

У плані реалізації такого адаптивного підходу управління безпекою, пропонується використовувати концепцію, відповідно до якої виконуються такі процедури [2, 5, 6] (рис. 2):

– оцінка заданого аттрактивного стану системи;

– генерація структури, межі якої визначають множини "нормальних станів КІВУСКЗ»;

– рекурсивна верифікація аттрактивного стану системи;

– оцінка чутливості системи до зовнішніх впливів;

– адаптація до виявлених порушень безпеки.

Верифікація «нормального стану КІВУСКЗ» дозволяє встановити простір станів, в якому гарантовано виконуються вимоги безпеки, які пред'являються до системи.

У разі виявлення порушень безпеки сукупність зазначених процедур замикається, утворюючи робочий цикл адаптивного управління безпекою КІВУСКЗ [5]. Адаптація до порушень безпеки здійснюється шляхом ідентифікації, оцінки чутливості системи до зовнішніх впливів, прогнозування пове-

дінки системи та зміни її параметрів в залежності від причин порушень, встановлених за невиконання умов заданого аттрактивного стану системи. Виконання цих дій гарантує побудову повної множини досяжних станів КСКП, прогнозування зміни властивості безпеки по станам системи в майбутньому і цільну доказову безпеку системи відповідно до поставленої оптимізаційної задачі.

У загальному вигляді управління безпекою КІВУСКЗ може бути представлено послідовністю дій, наведеною на рис. 2.

Рис. 2. Блок-схема адаптивного управління безпекою КІВУСКЗ

Спочатку для КІВУСКЗ задається аттрактивний стан системи (рис. 2, етап 1), шляхом опису структури, межі якої визначають множини "нормальних станів КІВУСКЗ». Прикладом такого опису може бути аттрактор спостережуваного структурно-інформаційного портрета межі якого свідчать про безпеку КІВУСКЗ. Множина таких аттракторів вимагає попереднього завдання з урахуванням правил розподілу доступу, реалізованих в моделях контролю доступу операційного середовища КІВУСКЗ та управління доступом на рівні мережевих пристроїв. Потім визначається показник безпеки КІВУСКЗ (рис. 2, етап 2), який є на безлічі параметрів системи індикатором її невиходу з встановленого режиму функціонування. Для сигналізації про порушення безпеки необхідно спрацьовування деякої індикаторної функції, яка задає правило обчислення значення даного показника.

На цьому підготовчі процедури завершуються. Після цього здійснюється фіксація зовнішнього впливу (рис. 2, етап 3) і, якщо такий вплив на КІВУСКЗ існує, то - фіксація стану КІВУСКЗ (рис. 2, етап 4). Знаючи стан КІВУСКЗ, потім можна виконувати власне процедури управління:

– оцінка чутливості системи до зовнішніх впливів (рис. 2, етап 5);

– верифікація «нормального стану КІВУСКЗ» (рис. 2, етап 6);

– визначення керуючого впливу, відповідного виявленим порушенням безпеки (рис. 2, етап 7);

– адаптація КІВУСКЗ (рис. 2, етап 8) з метою усунення (якщо порушення виявлено в поточному стані КІВУСКЗ) і запобігання (якщо порушення виявлені в досяжних станах КІВУСКЗ) порушень безпеки, виявлених на етапі верифікації «нормального стану КІВУСКЗ».

До складу пристрою управління входять наступні модулі:

"Виявлення впливу", який відстежує факт запиту та здійснення несанкціонованого впливу на систему;

"Стан безпеки системи", в який передається сигнал від модуля "Виявлення впливу" про вплив на стан КІВУСКЗ, який нещодавно стався, і який при надходженні цього сигналу виконує збір інформації про поточний стан параметрів;

"Опис заданого аттрактивного стану системи", який дозволяє перерахувати умови безпеки КІВУСКЗ і тим самим задати показник безпеки;

"Верифікація« нормального стану КІВУСКЗ »", який дозволяє на основі зафіксованого стану та заданих аттрактівних станів системи оцінити їх виконання;

"Виявлення причин порушень безпеки", який, у разі, якщо виявлено порушення системи, визначає причини порушень і виконує адаптацію до порушень шляхом ідентифікації і зміни необхідних параметрів КІВУСКЗ залежно встановлених причин.

За фактом впливу на поточний стан КІВУСКЗ, виконується фіксація параметрів, склад і значення яких визначаються або об'єктною моделлю операційного середовища КІВУСКЗ або спеціалізованим програмним забезпеченням. Потім у ході верифікації «нормального стану КІВУСКЗ» виконується оцінка показника безпеки. Якщо його значення індикує порушення безпеки, то визначається керуючий вплив на параметри. Для цього шляхом зіставлення множин поточних параметрів і заданих параметрів виявляються відсутні елементи цих множин по кожному з вимог і / або некоректно задані / відсутні значення параметрів.

Таким чином, розроблена модель адаптивного управління безпекою КІВУСКЗ, що враховує властивість внутрішнього міжелементного взаємозв'язку окремих компонент і підсистем.

2. Адаптивний метод виявлення зловмисних зовнішніх впливів на КІВУСКЗ на основі нейронних мереж

Аналіз процесу функціонування КІВУСКЗ показав, що зовнішнім впливам на нормально протікаючі процеси в КІВУСКЗ піддаються більшість її підсистем і елементів.

Проведені дослідження показали, що в даний час існує безліч можливих видів атак. Однак, як по-

казав досвід експлуатації КІВУСКЗ, найбільш часто зловмисники використовують чотири основні види: *DoS, MAC-flooding, R2L* та *Probe* [5].

Атака *DoS* – відмова в обслуговуванні, характеризується генерацією великого обсягу трафіку, що призводить до перевантаження і блокування сервера. Атака *MAC - flooding* відноситься до класу разведовательных атак, в який атакуюча машина забиває перемикач (switch) величезним числом кадрів з невірними MAC- адресами посилача. Атака *R2L* характеризується отриманням доступу незареєстрованого користувача до комп'ютера з боку видаленої машини. Атака *Probe* полягає в скануванні портів з метою отримання конфіденційної інформації.

Проведені дослідження показали, що виявлення і локалізацію наведених зловмисних вторгнень в систему можна здійснити, використовуючи для цього моделі і методи нейронних мереж. При цьому в якості вхідних даних для нейронних мереж повинні служити показники КІВУСКЗ, які характеризують поточний стан системи.

Досвід практичної експлуатації КСКП показав, що поточний її стан можна визначити за допомогою ряду внутрішніх параметрів, які в сукупності формують вектор внутрішніх станів системи (множина характеристик $X = (x_1, x_2, ..., x_n)$).

Крім того, в якості вхідних даних системи розподілу доступу і захисту інформації в КІВУСКЗ доцільно використовувати результати *BDS*-тестування [4] і параметри меж функції чутливості [5] (значення мінімуму і максимуму). В якості вихідних даних необхідно сформувати п'яти мірний вектор $Y = (y_1, y_2, \ldots, y_5)$, де п'ять - це кількість класів атак плюс нормальний стан.

Розглянемо нейромережевий підхід вирішення даної задачі, який полягає в послідовному об'єднанні двох різних нейронних мереж. На рис. 3 наведена система розпізнавання класів атак на основі багатошарового персептрона (*MLP*) [7]. На вхід системи подається вектор $X = (x_1, x_2, ..., x_{19})$, где $x_1, x_2, ..., x_{16}$ – характеристики системи, x_{17}, x_{18} – значення показників функції чутливості, x_{19} – значення *BDS*-тесту. Завданням такої системи є виявлення і розпізнавання атак.

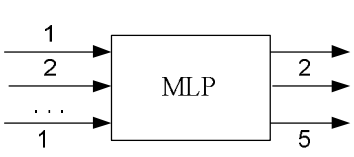

Рис. 3. Нейромережева система виявлення атак

Для виявлення та розпізнаванні атак пропонується використовувати багатошаровий перцептрон, який здійснює обробку стислого простору вхідних образів з метою розпізнавання класу атаки. При проектуванні системи слід враховувати, той факт що значення показників функції чутливості (x_{17}, x_{18}) і значення *BDS*-тесту (x_{19}) повинні мати вищій пріоритет прийняття рішення.

Для навчання і тестування системи виявлення комп'ютерних атак використовувалася 10% вибірка з бази KDD. Для навчання нейронних мереж були відібрані 8743 прикладів. Далі вся 10% вибірка застосовувалася для тестування. Результати тестування в режимі розпізнавання класу атаки наведені в табл. 1.

Таблиця 1

Результати тестування для комп'ютерних атак

Клас	Всього	Виявлено	Розпізнано
DoS	6487	6460 (99.58%)	6310 (97.27%)
MAC - flooding	52	50 (96.15%)	42 (80.77%)
R2L	943	929 (98.51%)	398 (42.20%)
Probe	1561	1387 (88.85%)	1329 (85.37%)
Нормальний стан	8743	---	8497 (97.19%)

Аналіз результатів дослідження показав, що найкращий результат був досягнутий для атак класу *DoS* і *Probe*. Дещо гірше визначаються *MAC - flooding* і *R2L*, відповідно 80,77% і 42,20%.

Таким чином, шляхом використання нейронних мереж, *MLP*, можна ідентифікувати і розпізнавати комп'ютерні атаки з досить високим ступенем точності. Основними перевагами використання підходів, заснованих на нейронних мережах, є здатність адаптуватися до динамічних змін стану КІВУСКЗ і швидкість розпізнавання атак, що особливо важливо при роботі системи в режимі реального часу.

3. Метод синтезу нейронних мереж для виявлення шкідливого програмного забезпечення

Дослідження методів впровадження, поширення та впливу зловмисного програмного забезпечення (ПЗ), а також систем захисту інформації від нього, показали високий ступінь їх взаємозалежності (впливу один на одного), при цьому рівень технічного і програмного забезпечення зловмисників у більшості практичних випадків вище. У зв'язку з цим існуючі засоби захисту КІВУСКЗ не завжди своєчасно справляються з ідентифікацією зловмисного ПЗ і його локалізацією в разі поширення епідемії. Саме тому в теперішній час актуальним завданням є розробка ефективних методів виявлення шкідливих програм, які здатні виявляти невідомі комп'ютерні шкідливі програми [3].

Розглянемо інтелектуальну систему виявлення комп'ютерних вірусів [1, 7], яка базується на застосуванні нейронних мереж. Така система використовує основні принципи функціонування біологічної імунної системи, де в якості окремого детектора використовується нейронна мережа. На рис. 4 представлена структура нейромережевої штучної імунної системи для виявлення зловмисного ПЗ [1].

Вона складається з таких основних модулів:

модуль генерації детекторів,

модуль навчання імунних детекторів,

модуль відбору детекторів,

модуль знищення детекторів,

модуль виявлення шкідливих програм,

модуль ідентифікації вірусів,

модуль клонування і мутації детекторів,

модуль формування імунної пам'яті.

Нейромережеві імунні детектори (НІД) відіграють одну з найбільш важливих ролей у виявленні зловмисного ПЗ. Пройшовши стадії навчання та відбору, детектори набувають здатність реагувати на шкідливі програми, скануючи їх структуру, і, в той же час, ігнорувати чисті файли [1, 7].

Функціонування НІД полягає в послідовності таких дій [1]:

1. Випадковим чином зі списку існуючих файлів нейромережевий імунний детектор вибирає файл для перевірки.

2. Дані з файлу проходять попередню обробку, пов'язану з видаленням «дірок» і незначущих нулів.

3. За методом ковзаючого вікна, детектор сканує файл і приймає рішення про належність файлу що перевіряється до класу чистих або до класу шкідливих програм.

4. Якщо нейромережевий імунний детектор приймає рішення про належність файлу що перевіряється до класу чистих програм, детектор вибирає новий файл для перевірки.

5. Якщо нейромережевий імунний детектор приймає рішення про належність файлу що перевіряється до класу шкідливих програм, він подає сигнал про виявлення комп'ютерного вірусу і нейромережна імунна система переходить в особливий режим функціонування.

На рис. 5 представлений нейромережевий імунний детектор. Він складається з нейронної мережі зустрічного поширення [1] і арбітра. Нейронні елементи прихованого шару функціонують за принципом «переможець бере все», тобто вихідне значення нейрона-переможця дорівнює «1», а вихідні значення решти нейронних елементів дорівнюють «0». Вихідне значення *j*-го нейрона третього шару визначається згідно з формулою:

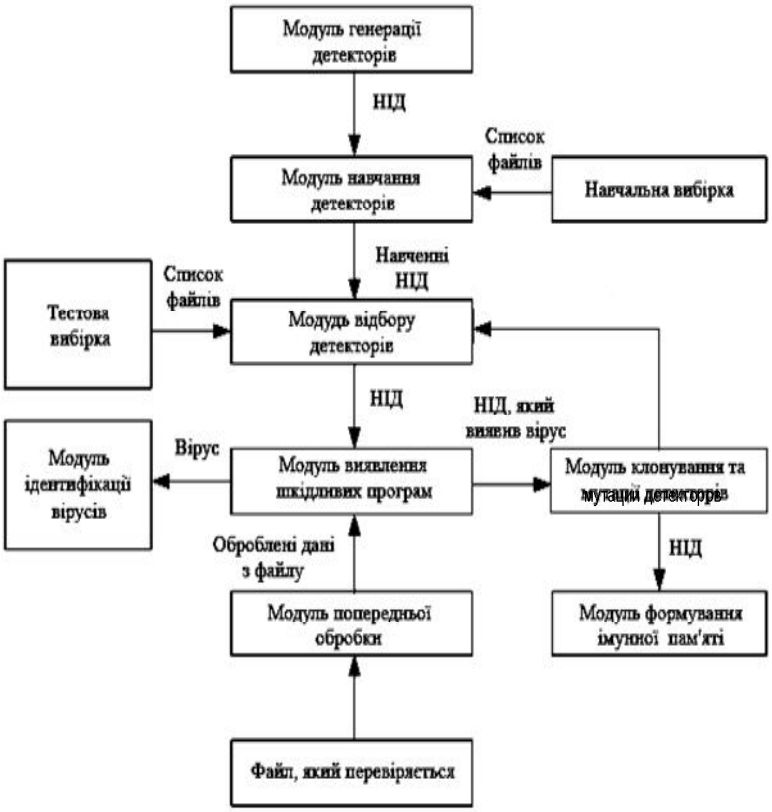

Рис. 4. Структура нейромережевої штучної імунної системи для виявлення шкідливих програм

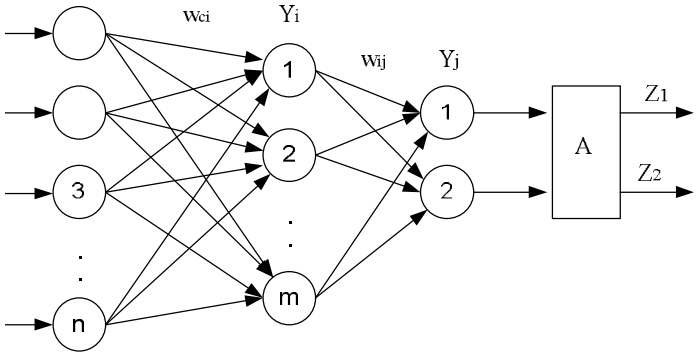

Рис. 5. Нейромережний імунний детектор

$$U_{вых}(Y_j) = \sum \omega_{kj} \cdot U_{вых}(Y_k). \qquad (4)$$

Арбітр приймає остаточне рішення про те, чи є сканируемий файл шкідливим. Для цього він обчислює кількість чистих і шкідливих фрагментів сканованого файлу

$$\overline{Y_1} = \sum_{k=1}^{L} Y_1^k, \qquad (5)$$

$$\overline{Y_2} = L - \overline{Y_1} = \sum_{k=1}^{L} Y_2^k, \qquad (6)$$

де L – множина образів сканованого файлу, Y_i^k – вихідне значення *i*-го нейрона лінійного шару при подачі на вхід мережі *k*-го образу.

Далі визначаються ймовірності належності сканованого файлу відповідно до нормального і аномального класу

$$P_T = \frac{\overline{Y_1}}{L} \cdot 100\%, \quad (7)$$

$$P_F = 1 - P_T = \frac{\overline{Y_2}}{L} \cdot 100\%, \quad (8)$$

Проведені дослідження та експертна оцінка показали, що остаточне рішення про належність файла до нормального класу арбітр приймає таким чином:

$$Z_1 = \begin{cases} 1, \text{ якщо } P_T > 90\%; \\ 0, \text{ інакше.} \end{cases} \quad (9)$$

Відповідно, рішення про належність сканованого файлу до аномального класу приймається у відповідності з таким виразом:

$$Z_2 = \begin{cases} 1, \text{ якщо } P_F > 10\%; \\ 0, \text{ інакше.} \end{cases} \quad (10)$$

Таким чином, простір вихідних значень арбітра можна представити у табличному вигляді (табл. 2).

Таблиця 2

Простір вихідних значень арбітра

Z_1	Z_2	клас
1	0	Нормальний
0	1	Аномальний
0	0	Не визначено

Порівняльний аналіз результатів виявлення невідомих шкідливих програм різними антивірусними програмами показав, що розроблений підхід, заснований на нейронній мережі, дозволяє якісніше детектувати невідомі шкідливі програми.

Висновки

Таким чином, розроблений комплекс методів адаптивного управління КІВУСКЗ, які на відміну від відомих, використовують інтелектуальний підхід до виявлення порушень безпеки на множині параметрів КІВУСКЗ, що дозволить вирішувати завдання виявлення причин деструктивних змін стану системи і контролю параметрів у відповідності з гарантованими вимогами безпеки та функціональної цілісності КІВУСКЗ.

Список літератури

1. Безобразов, С.В. Алгоритмы искусственных иммунных систем и нейронных сетей для обнаружения вредоносных программ / С.В. Безобразов, В.А. Головко // Научная сессия НИЯУ МИФИ «Нейроинформатика»: материалы Всеросс. науч. конф., МИФИ, Москва, 25-29 янв. 2010. – Москва, 2010. – С. 273-287.

2. Калинин М.О. Адаптивное управление безопасностью информационных систем на основе логического моделирования: дис. ... доктора техн. наук: 05.13.19 [Текст] / Калинин Максим Олегович. – Санкт-Петербург., 2010. – 308 с.

3. Касперский Е. Компьютерное зловредство/ Е. Касперский. – СПб.: Питер, 2007. – 208 с.

4. Кузнецов А.А. Метод структурной идентификации информационных потоков в телекоммуникационных сетях на основе BDS-тестирования / А.А. Кузнецов, С.Г. Семенов, С.М. Симоненко, Є.В. Мелешко // Наука і техніка Повітряних Сил Збройних Сил України. – Х.: ХУ ПС, 2010.– № 2 (4). – С. 131-136

5. Семенов С.Г. Анализ и синтез защищенных компьютерных систем и сетей / С.Г. Семенов, А.А. Подорожняк, А.И.Баленко. – Х:НТУ«ХПИ», 2012. – 188 с.

6. Семенов С.Г. Модели и методы управления сетевыми ресурсами в информационно-телекоммуникационных системах / С.Г. Семенов, А.А. Смирнов, Е.В. Мелешко. – Х.:НТУ«ХПИ», 2012. – 240 с.

7. Хайкин С. Нейронные сети: полный курс / С. Хайкин. – М.: Вильямс, 2006. – 1104 с

Надійшла до редколегії 24.01.2013

Рецензент: канд. техн. наук с.н.с. Г.А. Кучук, Харківський університет Повітряних Сил імені І. Кожедуба, Харків.

КОМПЛЕКС МЕТОДОВ АДАПТИВНОГО УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ КОМПЬЮТЕРИЗОВАННЫХ ИНФОРМАЦИОННО ИЗМЕРИТЕЛЬНЫХ УПРАВЛЯЮЩИХ СИСТЕМ КРИТИЧЕСКОГО ПРИЛОЖЕНИЯ

С.Г. Семенов, Н.Й. Заполовский, А.И. Баленко

В статье разработана модель адаптивного управления безопасностью компьютеризованных информационно измерительных управляющих систем критического приложения (КИВУСКЗ). Проведено исследование и разработан алгоритм выполнения процедур управления безопасностью КИВУСКЗ. На основе результатов исследования предложен комплекс методов адаптивного управления безопасностью КИВУСКЗ, которая включает в себя адаптивный метод выявления злоумышленных внешних влияний на КИВУСКЗ на основе нейронных сетей и метод синтеза нейронных сетей для выявления вредного программного обеспечения. Проведено исследование и получено результаты тестирования системы в условиях злоумышленных влияний компьютерных атак.

Ключевые слова: *компьютеризованная информационно-измерительная управляющая система критического приложения, компьютерные атаки, нейронные сети, нейросетевой иммунный детектор.*

COMPLEX OF METHODS OF ADAPTIVE CONTROL SAFETY COMPUTER-ASSISTED INFORMATIVELY THE MEASURINGS SENSOR-BASED SYSTEMS OF CRITICAL APPLICATION

S.G. Semenov, N.Y. Zapolovskiy, A.I. Balenko

In the article an adaptive case safety frame is developed computer-assisted informatively the measurings sensor-based systems of critical application (CAIMSBSCA). Research is conducted and the algorithm of implementation of procedures of management safety of CAIMSBSCA is developed. On the basis of results of research a complex is offered of methods of adaptive control safety of CAIMSBSCA, which plugs in itself the adaptive method of exposure of ill-intentioned external influences on CAIMSBSCA on the basis of neuron networks and method of synthesis of neuron networks for the exposure of harmful software. Research is conducted and the results of testing of the system are got in the conditions of ill-intentioned influences of computer attacks.

Keywords: *computer-assisted informatively-measuring sensor-based system of critical application, computer attacks, neuron networks, neuron net immune detector.*