УДК 004.75:004.5:004.49
DOI https://doi.org/10.32782/2663-5941/2023.3.1/34

Савенко Б.О.
Хмельницький національний університет

МЕТОД СИНТЕЗУ МАТЕМАТИЧНИХ МОДЕЛЕЙ РІВНІВ БЕЗПЕКИ ДЛЯ ЧАСТКОВО ЦЕНТРАЛІЗОВАНИХ РОЗПОДІЛЕНИХ СИСТЕМ ВИЯВЛЕННЯ ЗЛОВМИСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Зловмисники продовжують активно розробляти, використовувати і поширювати зловмисне програмне забезпечення. Особливо актуальним питанням щодо протидії зловмисному програмному забезпеченню є розробка методів засобів виявлення та протидії йому для використання в корпоративних мережах. Такі засоби повинні будуватись на нових методах та враховувати особливості таких архітектур в процесах протидії та виявлення зловмисного програмного забезпечення. Метою роботи є розробка методу синтезу математичних моделей рівнів безпеки для нових типів засобів виявлення зловмисного програмного забезпечення в корпоративних мережах. Розроблені засоби є самоорганізованими розподіленими системами з частковою централізацією. Часткова централізація як властивість системи означена так, що для прийняття рішення щодо подальших кроків системи, сукупність компонент, в яких міститься центр прийняття рішень системи, будуть розглядатись як децентралізована підсистема. Керування системою буде здійснювати центр прийняття рішень, який розподілений спочатку у визначених компонентах і може в процесі її функціонування змінювати місце знаходження в решті компонент. Для визначення станів компонент системи запропоновано характеристичні показники та розроблено узагальнені аналітичні вирази для їх обчислення. Ці характеристичні показники задають стани компонент розподіленої системи. В роботі узагальнено формування таких характеристичних показників компонент системи. Характеристичні показники можуть бути неперервними і дискретними величинами, тому для кожного випадку розроблено різні варіанти їх подання та обробки значень. Для здійснення узагальнення характеристичних показників розроблено метод синтезу математичних моделей рівнів безпеки. Такі обчислення дають змогу оцінити стан компонент в системі з метою самостійного визначення нею її подальших кроків. В результаті сформована система стає основою для наповнення її методами виявлення зловмисного програмного забезпечення в поєднанні з компонентами системи як цілісного сенсору. Для тестування системи було здійснено імплементацію в неї методу виявлення worm-вірусів та проведено експерименти. Результати експериментальних досліджень підтвердили ефективність запропонованого рішення.

Подальші дослідження будуть проведені для включення додаткових характеристичних показників ознак та реалізації в системі методів виявлення зловмисного програмного забезпечення.

Ключові слова: *часткова централізація, самоорганізація, зловмисне програмне забезпечення, worm-вірус, розподілена система.*

Постановка проблеми. Подальше активне використання і поширення зловмисного програмного забезпечення (ЗПЗ) [1, с. 1] продовжує створювати проблеми користувачам щодо вирішення задач в комп'ютерних системах та мережах (КСМ). Також, блокує доступ до КСМ та інформаційних ресурсів та для усунення наслідків вимагає витрат часу кваліфікованого персоналу. Використання антивірусних засобів (АВЗ) та систем виявлення вторгнень (СВВ) є досить ефективним. Але використовувані при створенні ЗПЗ нові методи дають змогу зловмисникам частково обходити такі засоби і це залишає їм простір для подальшої зловмисної діяльності. Крім того, робота АВЗ та СВВ потребує залучення користувача до процесу адміністрування подій, про які інформуватимуть ці засоби і системи у випадку виявлення ЗПЗ чи підозри на наявність ЗПЗ. А це призводитиме до витрат часу, особливо коли користувач не має відповідної кваліфікації. Практики із забезпечення безпеки та захисту КСМ відповідними АВЗ та СВВ підтверджують необхідність застосування комплексних систем, які б включали багаторівневість, багатоетапність та різноманітність. Різноманітність [2, с. 251] АВЗ та СВВ, якщо відомості про імплементовані в них методи виявлення невідомі зловмиснику, суттєво покращують безпеку та захист КСМ та їх ресурсів. Тому, потрібно використовувати нові типи засобів додатково до широко використовуваних.

Актуальними такі завдання забезпечення безпеки є для корпоративних мереж. В них викорис-

товуються різноманітні мережні системи виявлення ЗПЗ. Для виявлення ЗПЗ при проєктуванні таких систем виявлення потрібні показники з різних вузлів мережі та комп'ютерних станцій. Значення цих показників можуть бути використані при розробці методів виявлення ЗПЗ, а також першочергово для врахування їх при функціонуванні таких систем. Але опис таких характеристичних показників повинен базуватись аналітичних виразах для подальшого обчислення їх значень. Ці характеристичні показники можуть бути різними, їх кількість теж може бути різною для розв'язання різних задач, також, вони можуть бути визначені дискретними або неперервними функціями. Враховуючи таку різноманітність характеристичних показників потрібно їх узагальнити в контексті формування таких характеристичних показників компонент системи. Те, що вони можуть бути неперервними і дискретними величинами, то для кожного випадку потрібно розробити різні варіанти їх подання та обробки значень. Таким чином, актуальним для здійснення узагальнення характеристичних показників буде розробка методу синтезу математичних моделей рівнів безпеки. Такі обчислення дадуть змогу оцінити стан компонент в системі з метою самостійного визначення нею її подальших кроків. В результаті сформована система [2, с. 251; 3, с. 21] стане основою для наповнення її методами виявлення ЗПЗ в поєднанні з компонентами системи як цілісного сенсору. Ці показники будуть використані системою для перебудови її архітектури самостійно в залежності від стану безпеки в комп'ютерних станціях та в мережі.

Аналіз останніх досліджень і публікацій. Зловмисники продовжують створювати ефективне ЗПЗ і такі дії мають стійку тенденцію до зростання, як кількісно, так і за охопленням різних типів [4, 5]. Для корпоративних мереж використовуються відомі засоби, наприклад пропоновані в [6, 7], які є ефективними, але вони не забезпечують повного виявлення та надійної протидії ЗПЗ. Це підтверджується відповідними результатами незалежних антивірусних лабораторій та самими розробниками. Тому, є потреба в подальшій розробці нових систем та методів для виявлення ЗПЗ в корпоративних мережах, які повинні бути розподіленими. Проєкт, який подано в [8], є найбільш найближчим подібним рішенням, яке буде розглядатись в цій роботі і набуватиме подальшого розвитку.

Розглянемо розподілені системи та принципи їх створення [9, с. 1; 10, с. 1; 11, с. 49] для ефективного використання в комп'ютерних мережах, зокрема і ті, які спеціалізовані для виявлення ЗПЗ. У роботах [12, с. 57; 13, с. 743] пропонуються методи вирішення проблеми побудови орієнтованого мінімального остовного дерева для застосування при створенні розподілених систем. У роботі [14, с. 1] показано, як побудувати накладену мережу постійного ступеня та заданого діаметру за допустимий час, починаючи з довільного слабозв'язного графа. В роботі [15, с. 107] проаналізовано синхронну динаміку k-більшості, де в кожному круглому вузлі з дискретним часом рівномірно випадковим чином відібрано k сусідів із заміною. В роботі [16, с. 1] проаналізовано паралельні обчислення як особливу тісно пов'язану форму розподілених обчислень, і розподілені обчислення розглядаються як слабко пов'язану форму паралельних обчислень. Розширення цього поняття на інтернет речей подано в роботі [17, с. 684]. В роботах [18, с. 318, 19, с. 17] представлено теорію, що використовується для моделювання конкретного класу розподілених великомасштабних систем. Використання наукових результатів дослідників, які подані в роботах [9, с. 1; 10, с. 1; 11, с. 49; 12, с. 57; 13, с. 743; 14, с. 1; 15, с. 107; 16, с. 1; 17, с. 684; 18, с. 318; 19, с. 17], потрібно при створенні розподілених систем в корпоративних мережах. Всі проаналізовані рішення можуть бути використані в проєктованій системі з характеристиками, які подані в роботах [2, с. 251; 3, с. 21].

Враховуючи, що пошук та виявлення ЗПЗ потрібно здійснювати в корпоративній мережі, то актуальними для розгляду будуть такі: мережні IPS (Network – based Intrusion Prevention, NIPS) [20]; IPS для бездротових мереж (Wireless Intrusion Prevention Systems, WIPS) [21]; системи для здійснення поведінкового аналізу мережі (Network Behavior Analysis, NBA) [22]. Наукові праці, які містять методи побудови розподілених систем та методи виявлення ЗПЗ подано в [23, с. 127; 24, с. 166].

Розглянемо об'єктами ЗПЗ таку його підмножину, як worm-віруси. В роботах [25, с. 405; 26, с. 1319] представлено декомпозицію вірусів і worm-програм на основі їх основних функціональних компонентів. В роботі [27, с. 1] здійснено аналіз троянського коня, який під час виконання може змінювати інші комп'ютерні програми, наприклад, копіюючи себе (або його частину) у них. В роботі [28, с. 78] зловмисні програми аналізуються на наявність ознак вірусів, worm-вірусів, троянських програм і руткітів

та конкретні контрзаходи, для їх розпізнавання. У роботі [29, с. 247] побудовано модель SIQR для розповсюдження worm-вірусу залежно від двофакторної моделі. У роботі [30, с. 1] зроблено припущення про існування так званих багатовекторних worm-вірусів. В ній подано пару з них за слідами нападу, які зібрані в приманці. У роботі [31, с. 213] проаналізовано приклади ЗПЗ: віруси, worm-віруси, троянські програми, шпигунське програмне забезпечення, клавіатурні шпигуни, ботнети, руткіти, програмне забезпечення для вимагання та випадкові завантаження. Різноманітність ЗПЗ проявляється згідно проведеного аналізу наукових результатів [25, с. 405; 26, с. 1319; 27, с. 1; 28, с. 78; 29, с. 247; 30, с. 1; 31, с. 213] не тільки за різнотиповістю основних підмножин, але і в межах певних класів та підмножин, зокрема, наприклад, багатовекторність worm-вірусів.

Тому, розробка методів і засобів виявлення ЗПЗ та протидії йому залишається актуальною проблемою сьогодення. Для створення нових типів систем виявлення ЗПЗ в корпоративних мережах за архітектурою та наповненням актуальним завданням є формування множини показників з вузлів мережі та їх ефективне визначення. Такі характеристичні показники будуть основою при прийнятті рішень системою.

В зв'язку з цим, **мета роботи полягає у** розробці методу синтезу математичних моделей рівнів безпеки для частково розподілених систем [2, с. 251; 3, с. 21] виявлення ЗПЗ, що дасть можливість узагальнити характеристичні показники та їх отримання, які необхідні для прийняття рішення системою виявлення.

Виклад основного матеріалу. Засоби систем виявлення ЗПЗ в комп'ютерних мережах, а також в їх хостах, повинні базуватись не тільки на сучасних актуальних методах виявлення, але і бути імплементованими в такі архітектури засобів, які б залучали свої елементи до покращення виявлення сумісно із методами виявлення. Реагування систем виявлення ЗПЗ в комп'ютерних мережах завдяки динамічній перебудові своїх архітектур в умовах зловмисних впливів та аномальних проявів створює додаткові перешкоди для зловмисників та ЗПЗ. Така динамічна перебудова архітектури повинна координуватись та узгоджуватись із застосуванням методів виявлення. Створення для зловмисників та ЗПЗ перешкод в розумінні функціонування та поведінки засобів виявлення на архітектурному рівні надає перевагу користувачам КСМ. Досягнення переваги потребує крім методів, які орієнтовані безпосередньо на виявлення ЗПЗ, забезпечити в складі засобів виявлення компоненти або елементу, які змінюватимуть архітектуру системи виявлення сумісно з методами виявлення, але при цьому вони не орієнтовані саме на виявлення конкретних типів ЗПЗ чи конкретного ЗПЗ. Такі компоненти чи елементи повинні забезпечувати функціонування системи виявлення ЗПЗ без втручання адміністратора системи чи користувача при прийняті рішень щодо подальшого функціонування в умовах впливів ЗПЗ і не бути прогнозованими в своїх подальших діях для зловмисників та користувачів.

Розглянемо такий тип систем виявлення ЗПЗ в комп'ютерних мережах, як частково централізовані системи [2, с. 251; 3, с. 21]. До таких систем віднесеио ті, в яких всі компоненти поділені на дві підмножини: підмножину компонент, в яких може бути центр системи; підмножину компонент, в яких відсутні функції для забезпечення функціонування центру прийняття рішень системи. Керування всією системою S відбувається з компонент, в яких знаходиться центр прийняття рішень системи. Тому, вона централізована. Часткова централізація забезпечується тим, що компоненти системи S, в яких знаходиться центр прийняття рішень системи для прийняття рішень формують пропозиції окремо в кожній з цих компонент, тобто децентралізовано, і погоджують його сумісно усі. Таким чином, система не повністю централізована.

Модель архітектури M_S частково централізованої системи S задамо згідно її компонентів та зв'язків між ними так:

$$M_S = \langle S, G_S \rangle, \qquad (1)$$

де G_S – граф (рис. 1), що відображає зв'язки між компонентами частково централізованої системи S.

Враховуючи поділ компонент системи на дві підмножини за критерієм наявності центру в них і без нього, отримуємо уточнену модель архітектури $M_{S,k}$ частково централізованої системи S згідно формули:

$$M_{S,k} = \langle\langle S_1, S_2, \ldots, S_k, S_{k+1}, S_{k+2}, \ldots, S_N, G_S \rangle, \qquad (2)$$

де G_S – граф (рис. 1), що відображає зв'язки між компонентами частково централізованої системи S; k – кількість компонент системи, в яких може бути центр прийняття рішень системи; $S = S_1 \cup S_2 \cup \ldots \cup S_k \cup \ldots \cup S_N$; N – кількість компонент в системі, які встановлені в комп'ютерні станції в мережі.

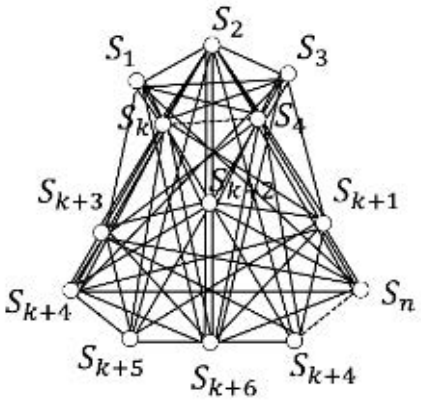

Рис. 1. Частково централізована архітектура системи

В запропонованій, таким чином, моделі архітектури $M_{S,k}$ частково централізованої системи, крім розподілу компонент системи, які задано підмножинами і відповідно вершинами, в залежності від можливостей містити центр, виділено також три типи зв'язків між компонентами, які поєднують компоненти з центром системи, компоненти без центру прийняття рішень системи та компоненти з центром і без центру між собою. Граф G_S при такому заданні є повним, тобто з'єднання між компонентами системи наявні між ними усіма. Але для ефективнішої роботи та приховування можливостей системи з'єднання між компонентами системи можуть бути задані різними деревами графа G_S і, таким чином, їх кількість зменшиться, а також, приховуватимуться від зловмисника або ЗПЗ очікувані повідомлення. Визначення варіантів дерев графа G_S встановлюватиметься центром прийняття рішень системи. Розроблена архітектура частково централізованих систем, архітектура її компонент та математичні моделі характеристичних показників рівнів безпеки компонентів є основою створення нових засобів виявлення ЗПЗ в корпоративних мережах, які та функціонування яких будуть невідомі або важко зрозумілі для зловмисників.

Для підтримки функціонування системи, враховуючи її специфіку застосування та потребу імплементації в неї принципів самоорганізації та адаптивності, потрібно в кожній компоненті визначати довіру до результатів обчислень та стан безпеки в ній. Тоді, задамо характеристичні показники значень рівнів безпеки компонентів множиною $B = \{\beta_1^{'}, \beta_2^{'}, \ldots, \beta_{N_B}^{'}\}$, де $\beta_i^{'}$ - значення рівнів безпеки компонентів системи, N_B – кількість характеристичних показників, $i = 1, 2, \ldots, N_B$. Для кожного компонента системи S введемо множини $B_j = \{\beta_{1,j}^{'}, \beta_{2,j}^{'}, \ldots, \beta_{N_B,j}^{'}\}$ згідно заданої множини B, елементи якої будуть використані для обчислення значення рівня безпеки всієї системи. Значення $\beta_{i,j}^{'}$ ($i = 1, 2, \ldots, N_B$) визначатимуть рівень довіри до результатів розподілених обчислень, які здійснені в різних компонентах системи та характеризують різні показники рівнів безпеки. Введемо для значень $\beta_{i,j}^{'}$ ($i = 1, 2, \ldots, N_B$; $j = 1, 2, \ldots, N$; N – кількість компонент в системі, які встановлені в комп'ютерні станції в мережі) проміжок, в якому буде регулюватись нижня межа в залежності від параметру рівня значущості $\alpha_z^{r,i}$ ($i = 1, 2, \ldots, N_B$; $z = 1, 2, \ldots, N_z$; N_z – кількість варіантів взаємодії функцій-підмножин) так: $\left[1 - \alpha_z^{r,i}; 1\right]$. За рівень значущості приймемо частку від одиниці, яка відображатиме відхилення від рівня довіри до результатів розподілених обчислень внаслідок певних подій, архітектурної особливості компоненти тощо. Для двох значень з проміжку $\left[1 - \alpha_z^{r,i}; 1\right]$ приймемо за значення з більшим рівнем довіри до результатів обчислень те, яке є більшим. Кожна компонента системи сформована з певної кількості функцій-підмножин в залежності від визначеного призначення компоненти. Для визначення значень $\beta_{i,j}^{'}$ ($i = 1, 2, \ldots, N_B$; $j = 1, 2, \ldots, N$; N – кількість компонент в системі, які встановлені в комп'ютерні станції в мережі) враховувати наявність центру прийняття рішень системи та типи обчислень, які можуть відноситись до різних груп функцій-підмножин та їх комбінацій. Характеристичні показники значень рівнів безпеки компонентів можуть бути різними і не завжди типовими. Тому, для їх формалізації з метою оцінювання потрібно застосовувати різні варіанти.

Якщо характеристичний показник за певним критерієм чи декількома критеріями може формуватись мінімум з двох однотипних елементів, тоді формуємо множину з цих елементів. Далі елементи впорядковуємо за їх впливом на безпеку компоненти і з них формуємо вектор, координати якого впорядковані. Потім конструюємо функцію, в якості аргументів якої будуть координати вектору, для відображення аргументів у значення з проміжку $\left[1 - \alpha_z^{r,i}; 1\right]$. В результаті отримані значення будуть значеннями характеристичних показників рівнів безпеки компонент. Ці значення можуть бути уточненні за певними показниками, які впливатимуть на безпеку. Такими показниками можуть бути функції-підмножини (кількість, призначення, активність, використання при виконанні завдань тощо), кількість компонент системи (активних, належних до центру прийняття рішень системи тощо). Коригування значення характеристичних показників здійснюємо введенням

коефіцієнта коригування, який враховує додаткові показники, що отримуються кількісними числовими значеннями. Цей коефіцієнт коригує рівень значущості $\alpha_z^{r,i}$ таким чином, щоб отримане значення характеристичного показника належало проміжку $\left[1-\alpha_z^{r,i};1\right]$.

Якщо характеристичний показник за певним критерієм чи декількома критеріями може бути заданий кількісними значеннями, тоді його значення потрібно задати залежним від цих кількісних значень з подальшим відображенням його в проміжок $\left[1-\alpha_z^{r,i};1\right]$. Коефіцієнт коригування цього значення не задаємо, бо він буде збіжним з коефіцієнтом при рівні значущості $\alpha_z^{r,i}$.

Якщо характеристичний показник за певним критерієм чи декількома критеріями повинен формуватись з декількох різних та різнотипних показників, тоді вважатимемо їх локальними складовими частинами та здійснюватимемо визначення значення характеристичного показника рівня безпеки компонент як середньоарифметичне або середньозважене значення серед всіх значень локальних показників так, щоб це значення належало проміжку $\left[1-\alpha_z^{r,i};1\right]$. При цьому для всіх значень локальних показників визначаємо локальні рівні значущості, які визначатимуть як середньоарифметичні або середньозважені значення рівні значущості $\alpha_z^{r,i}$. Локальні значення характеристичних показників належатимуть проміжкам $\left[1-\alpha_z^{r,i,l};1\right]$, де $\alpha_z^{r,i,l}$ – локальні рівні значущості.

З метою уникнення випадків, коли для декількох різних показників в одній чи різних компонентах системи S або щодо певної конкретної функції-підмножини можуть бути однаковими середньоарифметичні значення, потрібно при визначеннях таких значень враховувати початкове формування динамічних компонентів системи з різних функцій-підмножин, які можуть бути в різних компонентах. Особливо такі випадки в частині визначення середньоарифметичного значення коефіцієнта для рівня значущості, який дорівнюватиме 0,5 і, відповідно, значення характеристичних показників розподілятимуться на проміжках $\left[1-\alpha_z^{r,i};1\right]$ згідно рівномірного розподілу, можуть стосуватись дискретних величин, які потрібно задати числовими значеннями. Якщо формується вектор з характеристичних показників, які задано якісними показниками елементів однієї множини, тоді сформовані числові значення таких показників на проміжку будемо розміщувати не рівномірно через однакові інтервали, а з врахуванням певної ваги, яку визначатимемо коригуючим коефіцієнтом $\gamma_{F,1}$, що враховуватиме кількість та особливість функцій-підмножин в усіх компонентах системи. Визначимо коефіцієнт впливу кількості підмножин-функцій в усіх компонентах в залежності від того, як вони формують динамічні компоненти, так:

$$\delta_{1,F}=\sum_{i=1}^{n}\frac{\sum_{j=1}^{n_{F,S_i}}n_{F,S_i,j,0}}{\sum_{j=1}^{n_{F,S_i}}n_{F,S_i,j}}, \qquad (3)$$

де n_{F,S_i} – кількість функцій-підмножин в S_i компоненті; $n_{F,S_i,j}$ – покажчик наявності функції-підмножини в динамічній компоненті, причому як наявної безпосередньо в компоненті так і з решти компонент; $n_{F,S_i,j,0}$ – покажчик наявності функції-підмножини в динамічній компоненті не наявної безпосередньо в компоненті, а саме з решти компонент.

Визначимо, також, коефіцієнт впливу кількості підмножин-функцій в певних конкретних S_i компонентах в залежності від того, як вони формують динамічні компоненти, так:

$$\delta_{2,F,S_i}=\frac{\sum_{j=1}^{n_{F,S_i}}n_{F,S_i,j,0}}{\sum_{j=1}^{n_{F,S_i}}n_{F,S_i,j}}, \qquad (4)$$

де n_{F,S_i} – кількість функцій-підмножин в S_i компоненті; $n_{F,S_i,j}$ – покажчик наявності функції-підмножини в динамічній компоненті, причому як наявної безпосередньо в компоненті так і з решти компонент; $n_{F,S_i,j,0}$ – покажчик наявності функції-підмножини в динамічній компоненті не наявної безпосередньо в компоненті, а саме з решти компонент.

Визначатимемо коригуючим коефіцієнтом $\gamma_{F,1}$, що враховуватиме кількість та особливість функцій-підмножин в усіх компонентах системи так:

$$\gamma_{F,1}=\left(1-\delta_{1,F}\right)^d, \qquad (5)$$

де d – кількість характеристичних показників у векторі.

Значення коригуючого коефіцієнту $\gamma_{F,1}$ використовуватимемо для формування розподілу на характеристичних показників на відрізку $\left[1-\alpha_z^{r,i};1\right]$.

Аналогічно, визначатимемо коригуючий коефіцієнт $\gamma_{F,2}$, що враховуватиме кількість та особливість функцій-підмножин в усіх компонентах системи так:

$$\gamma_{F,2}=\left(1-\delta_{2,F}\right)^d, \qquad (6)$$

де d – кількість характеристичних показників у векторі.

Значення коригуючого коефіцієнту $\gamma_{F,2}$ використовуватимемо для формування розподілу на характеристичних показників на відрізку $\left[1-\alpha_z^{r,i};1\right]$.

Якщо $\delta_{1,F}$ чи $\delta_{2,F}$ дорівнюють нулеві, тобто всі функції-підмножини знаходяться в компонентах, то отримуємо значення коригуючих коефіцієнтів такими, що дорівнюють одиниці і, відповідно, рівномірний розподіл.

Якщо наявна кореляція певних характеристичних показників між собою, тоді потрібно встановити ступінь кореляції та виразити цю взаємну залежність аналітичним виразом. В зв'язку з таким випадком певні значення характеристичних показників можуть визначатись через аналітичні вирази певних корельованих з ним характеристичних показників.

Отримані значення характеристичних показників рівнів безпеки компонентів будуть задані аналітичними виразами.

Якщо характеристичні показники рівнів безпеки компоненти заданою множиною елементів і ці елементи впорядковані в координатах вектору та введена функція ранжування, тоді потрібно визначити найбільше і найменше значення з координат вектору, встановити крок для унормовуваних значень з проміжку найбільшого і найменшого значення з координат вектору, задати функцію відповідності унормованих значень з врахуванням одного з коригуючих коефіцієнтів $\gamma_{F,1}$ чи $\gamma_{F,2}$ в залежності від відношення до компонент чи компоненти в проміжок $\left[1-\alpha_z^{r,i};1\right]$ та задати аналітичний вираз обчислення значень характеристичних показників рівнів безпеки компонентів в різних компонентах системи S так:

$$\beta_{i,j}^{'} = 1 - \mu \cdot \alpha_z^{r,i}, \qquad (7)$$

де μ – коефіцієнт коригування, при якому більше з двох значень вказує на менший рівень безпеки компонент; $\mu \in [0,1]$; $\alpha_z^{r,i}$ – i-тий рівень значущості; $i = 1,2,\ldots,N_B$; $z = 1,2,\ldots,N_z$; N_z – кількість варіантів взаємодії функцій-підмножин; N_B – кількість характеристичних показників.

Якщо характеристичні показники за певним критерієм чи декількома критеріями задано кількісними значеннями, тоді їх значення потрібно задати аналітичним виразом залежним від цих кількісних значень з відображенням його в проміжок $\left[1-\alpha_z^{r,i};1\right]$ за формулою (6). Якщо характеристичні показники за певним критерієм чи декількома критеріями спочатку можна задати з декількох різних та різнотипних локальних показників, тоді визначити значення характеристичних показників рівня безпеки компонент як середньоарифметичні або середньозважені значення серед всіх значень відповідних локальних показників так, щоб ці значення належали проміжкам $\left[1-\alpha_z^{r,i};1\right]$ і локальні рівні значущості визначити, також, як середньоарифметичні або середньозважені значення рівні значущості $\alpha_z^{r,i}$, так:

$$\beta_{i,j}^{'} = \frac{1}{N_{B,i}} \cdot \sum_{w=1}^{N_{B,i}} \rho_w . \beta_{i,j,w}^{'} . \qquad (8)$$

де значення характеристичних показників рівні безпеки компонент $\beta_{i,j}^{'}$ належить проміжку $\left[1-\alpha_z^{r,i};1\right]$, $i = 1,2,\ldots,N_B$; N_B – кількість характеристичних показників; $j = 1,2,\ldots,N$; N – кількість компонент в системі, які встановлені в комп'ютерні станції в мережі; ρ_w – ваговий коефіцієнт для локальних значень $\beta_{i,j,w}^{'}$; $w = 1,2,\ldots,N_{B,i}$; $N_{B,i}$ – кількість локальних показників для i – того характеристичного показника; $\sum_{w=1}^{N_{B,i}} \rho_w = N_{B,i}$; для всіх $\rho_w = 1$ значення $\beta_{i,j}^{'}$ буде обчислене як середньоарифметичне; для всіх різних ρ_w значення $\beta_{i,j}^{'}$ буде обчислене як середньозважене; рівень значущості $\alpha_z^{r,i}$ для задання проміжку визначається з врахування локальних рівнів значущості $\alpha_z^{r,i,l,w}$: $\alpha_z^{r,i} = \frac{1}{N_{B,i}} \cdot \sum_{w=1}^{N_{B,i}} \rho_w . \alpha_z^{r,i,l,w}$.

Якщо наявна кореляція певних характеристичних показників між собою, тоді потрібно встановити ступінь кореляції та виразити цю взаємну залежність аналітичним виразом так:

$$\beta_{i,j}^{'} = \sum_{u=1}^{i-1} \sigma_u \cdot \beta_{u,j}^{'} + \sum_{u=i+1}^{N_B} \sigma_u \cdot \beta_{u,j}^{'}, \qquad (9)$$

де σ_u – частка від одиниці, яка виражає вагу кореляції значень $\beta_{u,j}^{'}$ та $\beta_{i,j}^{'}$; $u = 1,2,\ldots,N_B$; $u \neq i$.

Аналіз математичних моделей, які задано аналітичними виразами в формулах (3)-(8) за результатами проведеного експерименту з частково централізованою системою, підтверджує їх адекватність при застосуванні та коректність в граничних межах. Наприклад, в формулі (7) при відсутності чинників, які впливатимуть на безпеку процесів, що відбуваються в комп'ютерній станції в мережі, значення характеристичного показника $\beta_{i,j}^{'} = 1$, тобто коефіцієнт коригування $\mu = 0$. А при $\mu = 0$ значення характеристичного показника $\beta_{i,j}^{'} = 1 - \alpha_z^{r,i}$, що відповідає нижній межі проміжку $\left[1-\alpha_z^{r,i};1\right]$. Аналогічно, можна показати відповідність межам проміжку $\left[1-\alpha_z^{r,i};1\right]$ для решти результатів.

Отримані значення $\beta_{i,j}^{'}$ характеристичних показників рівнів безпеки в компонентах системи будуть використані для оцінювання результатів розподілених обчислень, отриманих з різних компонентів системи, з метою визначення ступеня довіри до них та подальшого використання центром прийняття рішень системи щодо наступних її кроків.

Функціонування частково розподілених систем згідно принципів самоорганізації та адаптивності забезпечується не тільки організацією комунікації між їх компонентами чи виконанням певних

спеціально орієнтованих завдань для виконання яких вони створені, але першочергово внутрішніми механізмами, методами та алгоритмами, які дадуть таким системам можливості вирішувати поставлені завдання без втручання користувача, самостійно приймати рішення щодо подальших кроків системи та адаптуватись в залежності під зміни зовнішнього середовища та внутрішніх подій.

Отримані значення характеристичних показників будуть використані центром прийняття рішень системи [2, с. 251] при визначенні її подальших кроків, але при цьому будуть поєднані разом із методом виявлення ЗПЗ в цій системі. В дану систему було імплементовано методи виявлення файлового ЗПЗ, який базовано згідно класифікації функцій прикладного програмного інтерфейсу. При виявленні ЗПЗ в одній з компонент системи і підтвердженні центром прийняття рішень, данні про нього розсилаються решті компонент.

Результати експериментальних досліджень. Розглянемо визначення ступеня стійкості системи S в процесі її функціонування з врахуванням специфіки виконуваних нею завдань. Стійкість системи S будемо досліджувати в контексті її можливості продовжувати своє функціонування і виконання поставлених завдань в умовах змін в середовищі функціонування, які зумовлені внутрішніми процесами самої системи та зовнішніми процесами, що можуть бути викликані різними причинами, зокрема зловмисним програмним забезпеченням, з мінімальною зміною чи втратою її функційності. Стани системи S, в яких вона буде функціонувати за відсутності впливів на неї ззовні і впливів, які будуть пов'язані з надійністю функціонування комп'ютерних станцій в корпоративній мережі, в які встановлені компоненти системи і які впливатимуть на внутрішні процеси в ній, включаючи і встановлення надійного зв'язку між ним, віднесемо до стану рівноваги всієї системи. Решту станів системи S віднесемо до нестійкого. Серед станів рівноваги виділимо стани часткової рівноваги, до яких віднесемо ті, в яких система S активуватиме методи виявлення ЗПЗ в комп'ютерній мережі. Тоді, фактично система може бути в трьох станах, переходи між якими і стани можна задати повним графом. Стан рівноваги системи зумовлений відсутністю впливів на неї збурюючих чинників. Стан часткової рівноваги зумовлений відсутністю впливів на неї збурюючих чинників і, при цьому, активізацією підсистеми для виявлення ЗПЗ. Стійкість системи S будемо характеризувати її здатністю повертатись до стану рівноваги після завершення перебування в стані часткової рівноваги або в нестійкому стані. Систему, в якій внаслідок впливу чинників вібувається віддалення від стану рівноваги або стану часткової рівноваги і, при цьому, вона тривалий час перебуває в нестійкому стані та не може перейти до інших станів, вважатимемо нестійкою.

Розглянемо умови стійкості системи S. Для кожного початкового значення, яке буде оброблятись, система повинна формувати результат, що не буде залишати її або в стані рівноваги або в стані часткової рівноваги. Якщо є протягом певного часу система S не отримує вхідних значень, тоді вона не формує жодних рішень. Так задані умови стійкості системи збіжні із заданими умовами її функціонування в комп'ютерних мережах згідно методу організації функціонування частково розподілених систем. Тоді, такі умови будемо вважати такими, що відповідають внутрішнім принципам функціонування системи і їх дотримання та аналіз можуть бути основою для дослідження стійкості системи в частині її стабільного функціонування. Показник стабільності буде встановлено для конкретної характеристики впливу. Для системи S характерною буде динамічна стійкість, яка відображає здатність до відновлення початкового стану після впливу чинників. Система S через наявність різних станів компонентів буде мати велику кількість варіантів в компонентів, тому розглядатимемо її як нелінійну динамічну систему.

Систему S будемо розглядати як самоорганізовану дискретну систему, оскільки вона перебуватиме в станах в залежності від станів її компонент. Використаємо для дослідження стабільності системи S узагальнені характеристичні показники значень рівнів безпеки компонентів, які задано множиною $B = \{\beta_1', \beta_2', \ldots, \beta_{N_B}'\}$, де β_i' – значення рівнів безпеки компонентів системи, N_B – кількість характеристичних показників, $i = 1, 2, \ldots, N_B$. Для кожного компонента системи S введемо підмножини $B_j = \{\beta_{1,j}', \beta_{2,j}', \ldots, \beta_{N_B,j}'\}$ згідно заданої множини B, елементи якої будуть використані для обчислення значення рівня безпеки всієї системи. Значення $\beta_{i,j}'$ ($i = 1, 2, \ldots, N_B$) визначатимуть рівень довіри до результатів розподілених обчислень, які здійснені в різних компонентах системи та характеризують різні показники рівнів безпеки. Введемо для значень $\beta_{i,j}'$ ($i = 1, 2, \ldots, N_B$; $j = 1, 2, \ldots, N$; N – кількість компонент в системі, які встановлені в комп'ютерні станції в мережі) проміжок, в якому буде регулюватись нижня межа в залежності від параметру рівня значущості $\alpha_z^{r,i}$ ($i = 1, 2, \ldots, N_B$; $z = 1, 2, \ldots, N_z$; N_z – кількість варіантів взаємодії функцій-підмножин) так: $\left[1 - \alpha_z^{r,i}; 1\right]$.

За рівень значущості приймемо частку від одиниці, яка відображатиме відхилення від рівня довіри до результату розподілених обчислень внаслідок певних подій, архітектурної особливості компоненти тощо. Тоді, якщо розглянути два характеристичних показники однієї компоненти, наприклад $\beta'_{1,j}, \beta'_{2,j}$ для j – ої компоненти, то результати обчислень можна відобразити на координатній площині двома точками. Якщо компонента системи функціонує стабільно, то значення точок міститимуться в прямокутнику, що задаватиметься по осі абсцис відрізком $\left[1-\alpha_z^{r,1};1\right]$ і по осі ординат відрізком $\left[1-\alpha_z^{r,2};1\right]$.

Задамо елементи множини B координатами вектору. В результаті отримаємо простір стану з різними векторами і їх значеннями. Відобразимо отримання цих значень в структурній схемі системи S на рис. 2.

Задамо функцію $W_{S,c}^1$ для опису блоку центру прийняття рішень системи так:

$$W_{S,c}^1 = \sqrt{\sum_{i=1}^{N_B}\sum_{j=1}^{N}\beta'^{\,2}_{i,j}}, \qquad (10)$$

де N_B – кількість характеристичних показників, $i = 1,2,\ldots,N_B$; $\beta'_{i,j}$ $(i = 1,2,\ldots,N_B)$ значення, які визначатимуть рівень довіри до результатів розподілених обчислень, що здійснені в різних компонентах системи та характеризують різні показники рівнів безпеки; $j = 1,2,\ldots,N$; N – кількість компонент в системі, які встановлені в комп'ютерні станції в мережі.

Значення функції $W_{S,c}^1$ буде відрізком, довжина якого не перевищуватиме значення $\sqrt{N_B \cdot N}$, і характеризуватиме стан системи коли увімкнені всі комп'ютерні станції та активні в них всі компоненти системи S. Нижньою межею значення функції $W_{S,c}^1$ буде $\sqrt{N \cdot \sum_{i=1}^{N_B}\left(1-\alpha_z^{r,i}\right)^2}$. Геометричною інтерпретацією функції $W_{S,c}^1$ буде точка в $N_B \cdot N$ – просторі з кількість координат $N_B \cdot N$. Тому, стабільність системи S буде залежати від значення функції $W_{S,c}^1$. Якщо значення буде перевищуватиме значення $\sqrt{N_B \cdot N}$, то система перейде до стану нерівноваги і буде вилучати компоненти з своєї архітектури, в яких найбільший вплив на значення функції $W_{S,c}^1$. Після таких вилучень компонент, система S повернеться до стану рівноваги і пробуватиме знову поетапно додавати компоненти. Якщо значення частини компонент дорівнюватимуть нулеві через їх відсутність в системі (вимкнені комп'ютерні станції), то значення функції $W_{S,c}^1$ обчислюється для наявних компонент і, тоді, точка задається в просторі меншого розміру, ніж $N_B \cdot N$. При цьому обчислене значення функції $W_{S,c}^1$ буде знаходитись так само в тому ж проміжку. Якщо значення функції $W_{S,c}^1$ буде менше за число $\sqrt{N \cdot \sum_{i=1}^{N_B}\left(1-\alpha_z^{r,i}\right)^2}$, тоді система теж перейде до стану нерівноваги, але цей стан буде викликано значеннями характеристичних показників станів безпеки компонент, при обчисленні яких було отримано значення, які не належать хоча б одному з проміжків $\left[1-\alpha_z^{r,i};1\right]$, але яке настільки менше $1-\alpha_z^{r,i}$, що вплинуло на загальний результуючий показник, тому цю або ці компоненти система вилучає зі своєї архітектури. Але може бути так, що це значення не вплине на загальний показник, хоча воно буде менше заданого значення, тоді система буде залишатись в стані рівноваги і вирішуватиме питання щодо аналізу значення з компоненти та за потреби її вилучення з архітектури системи.

Ступінь стійкості системи S в процесі її функціонування, враховуючи специфіку виконуваних завдань будемо визначати коефіцієнтом $k_{W_{S,c}^1}$ згідно значення функції $W_{S,c}^1$, обчисленого за формулою (10), так:

$$k_{W_{S,c}^1} = \frac{\sqrt{\sum_{i=1}^{N_B}\sum_{j=1}^{N}\beta'^{\,2}_{i,j}}}{\sqrt{N_B \cdot N}}. \qquad (11)$$

Тоді, система S при значенні $\frac{\sqrt{\sum_{i=1}^{N_B}\left(1-\alpha_z^{r,i}\right)^2}}{\sqrt{N_B}} \le k_{W_{S,c}^1} \le 1$, коли значення всіх $\alpha_z^{r,i}$ є найбільш допустимими,

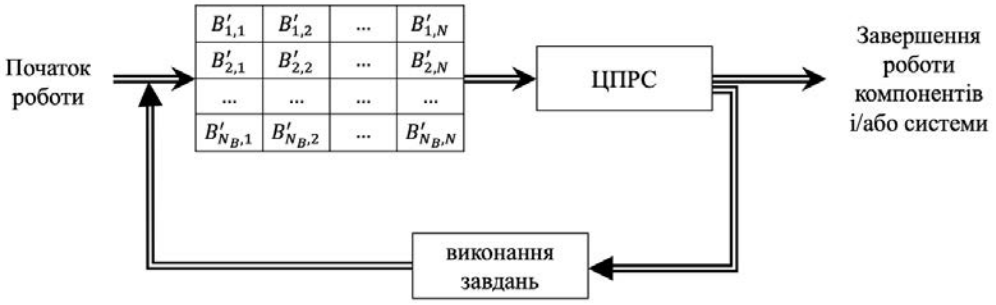

Рис. 2. Структурна схема системи S (ЦПРС – центр прийняття рішень системи)

буде перебувати в стані рівноваги і значення $k_{W^1_{S,c}}$ з цього проміжку буде критерієм стабільності для цієї системи. Коли частина компонентів системи S не буде активна через вимкнені комп'ютерні станції, то це теж впливатиме на стабільність її роботи і, відповідно, значення коефіцієнту буде меншим, бо враховуватиме потребу в усіх компонентах системи.

Проведемо експерименти з системою S для встановлення значення коефіцієнту стійкості при різних навантаженнях на систему і при різній архітектурі системі в частині кількості її компонент. Здійснимо постановку і проведення першого експерименту. Данні, які отримані в певний момент часу функціонування системи, були зафіксовані за таких умов: архітектура системи була сформована зі всіх 100 компонентів; підсистеми, які забезпечують виявлення ЗПЗ, не активізувались в системі за відсутності таких проявів. Тобто, за таких початкових встановлено, що система повинна функціонувати стабільно. Для проведення цього експерименту рівні значущості характеристичних показників було встановлено в залежності від їх важливості так:

1) $\alpha'_{1,S_i,1} = 0,01$, $\alpha'_{1,S_i,3} = 0,01$, $\alpha'_{2,S_{k+1,n},2} = 0,01$, $\alpha'_{2,S_{k+1,n},3} = 0,01$, $\alpha'_{2,S_{k+1,n},4} = 0,01$, $\alpha'_{2,S_{k+1,n},5} = 0,01$, $\alpha'_{3,S_{1,n},3} = 0,01$; 2) $\alpha'_{1,S_i,2} = 0,02$, $\alpha'_{3,S_{1,n},2} = 0,02$; 3) $\alpha'_{1,S_i,4} = 0,05$, $\alpha'_{1,S_i,5} = 0,05$, $\alpha'_{2,S_{k+1,n},1} = 0,05$, $\alpha'_{3,S_{1,n},1} = 0,05$, $\alpha'_{3,S_{1,n},4} = 0,05$, $\alpha'_{3,S_{1,n},5} = 0,05$.

За формулами (10) і (11) знаходимо значення функції $W^1_{S,c}$ та значення коефіцієнта стійкості системи $k_{W^1_{S,c}}$ і значення нижньої межі проміжку для коефіцієнту стійкості $\frac{\sqrt{\sum_{i=1}^{15}(1-\alpha_z^{r,i})^2}}{\sqrt{15}}$. Отримані значення $W^1_{S,c} = 38.214301635550662$, $k_{W^1_{S,c}} = 0.98668902547623$ і числове значення нижньої межі дорівнює 0.972848052541266 підтверджують перебування системи в стабільному стані.

Для проведення другого експерименту вимкнемо 30 комп'ютерних станцій. Отримуємо так само 15 таблиць, але в кожній з них буде мінімум тридцять нульових значень. Здійснюємо обчислення значень $W^1_{S,c} = 31.96599695772904$, $k_{W^1_{S,c}} = 0.825358492414677$ і числового значення нижньої межі, яке дорівнює 0.813943077452799. Результати підтверджують перебування системи в стабільному стані.

Третій експеримент проведемо при вимкнених 40 комп'ютерних станцій. Надамо додатково навантаження на певні показники і отримаємо сім числових значень більше одиниці. Проведемо обчислення значень $W^1_{S,c} = 29.58811566557844$, $k_{W^1_{S,c}} = 0.763961861456294$ і числового значення нижньої межі, яке дорівнює 0.753564861176528.

Таким чином, стабільність системи зменшується при зменшенні кількості активних компонент, бо кількість неактивних компонент враховується при оцінюванні стану всієї системи.

В комп'ютерних мережах може перебувати різноманітне ЗПЗ. При проведенні експериментів з системою S щодо достовірності виявлення ЗПЗ як об'єкти дослідження було розглянуто worm-віруси. Для оцінювання достовірності виявлення worm-вірусів системою S та імплементованим в неї методом, як цілісного бінарного класифікатора, визначено чутливість та специфічність моделі та обчислено їх значення. Значення чутливості $S_e = TPR = 73,5278\%$. Значення специфічності $S_p = 90,9274$.

Оскільки значення специфічності є високим, то система S виявляє негативні випадки краще, ніж позитивні, бо чутливість є меншою порівняно з специфічністю.

Висновки. В роботі запропоновано для визначення станів компонент частково централізованої системи [2, с. 251] використовувати характеристичні показники та розроблено метод синтезу математичних моделей рівнів безпеки, який дає змогу узагальнити отримання аналітичних виразів. Такі значення характеристичних показників компонентів системи та системи в цілому дають змогу оцінити стан компонент в системі з метою визначення нею її подальших кроків. Отримана таким чином система є основою для наповнення її методами виявлення ЗПЗ в поєднанні з компонентами системи як цілісного сенсору. Для тестування системи було імплементовано в неї метод виявлення worm-вірусів та проведено експерименти. Результати експериментальних досліджень підтвердили ефективність запропонованого рішення і, тому, запропоновані рішення щодо синтезу математичних моделей рівнів безпеки системи згідно часткової централізації можуть бути використані при створенні засобів виявлення ЗПЗ в корпоративних мережах.

Подальші дослідження будуть спрямовані на покращення самоорганізації системи та розробки методів виявлення ЗПЗ з наступною імплементацією їх в частково централізовані розподілені системи.

Список літератури:

1. США ліквідували шкідливе ПЗ Snake, за допомогою якого Росія 20 років шпигувала у країнах НАТО – Politico (zn.ua). URL: https://zn.ua/ukr/usa/ssha-likviduvali-shkidlive-prohramne-zabezpechennja-snake-za-dopomohoju-jakoho-rosija-20-rokiv-shpihuvala-v-krajinakh-nato.html

2. Савенко Б.О. Розподілена частково централізована система виявлення зловмисного програмного забезпечення в комп'ютерних мережах. *Актуальні проблеми комп'ютерних наук АПКН-2022* : матеріали XIV всеукр. наук.-практ. конф. (м. Хмельницький, 18-19 лист. 2022 р.). Хмельницький, 2022. С. 251-253. URL: https://kn.khmnu.edu.ua/wp-content/uploads/sites/18/apkn2022_corpuspaper.pdf

3. Савенко Б. О. Розподілені системи виявлення зловмисного програмного забезпечення. *2022 International Conference on Innovative Solutions in Software Engineering (ICISSE-2022)* : Conference Proceedings. (Ivano-Frankivsk, Ukraine, November 29-30, 2022) / Kuz M., Kozenko M. eds. Ivano-Frankivsk: VSPNU, 2022. Pp. 22-25. URL: https://shorturl.at/nyIMO

4. Security information portal Virus Bulletin, threat landscape. URL: https://www.virusbulletin.com/

5. The Independent IT-Security Institute. URL: https://www.av-test.org/en/

6. Symantec Enterprise Cloud - Broadcom Inc. URL: https://www.broadcom.com/products/cybersecurity

7. Symantec Product Categories. URL: https://sep.securitycloud.symantec.com/v2/landing

8. SNORT. Foremost Open Source Intrusion Prevention System. URL: https://www.snort.org/

9. van Steen M. R., Tanenbaum A. S. *Distributed Systems*. (3rd ed.). 2017. https://www.distributed-systems.net/index.php/books/distributed-systems-3rd-edition-2017/

10. Voulgaris S., Dobson M., and Steen M.van. Decentralized Network-level Synchronization in Mobile Ad Hoc Networks. *ACM Transactions on Sensor Networks*, Volume 12 (Issue 1), 2016, Article No. 5. Pp. 1-42. https://doi.org/10.1145/2880223

11. Czaja L. Distributed Systems–Objectives, Features, Applications. *Introduction to Distributed Computer Systems. Lecture Notes in Networks and Systems*. Springer, Cham. 2018. Vol 27. Pp. 49-64. https://doi.org/10.1007/978-3-319-72023-4_2

12. Fischer O., Oshman R. A distributed algorithm for directed minimum-weight spanning tree. *Distrib. Comput*. 2023. Vol. 36. Pp. 57–87. https://doi.org/10.1007/s00446-021-00398-3

13. Pandurangan G., Robinson P., Scquizzato M. A time- and message-optimal distributed algorithm for minimum spanning trees. *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing* (STOC). 2017. Pp. 743–756.

14. Götte, T., Hinnenthal, K., Scheideler, C. et al. Time-optimal construction of overlay networks. *Distrib. Comput.* 2023. Pp. 1-35. https://doi.org/10.1007/s00446-023-00442-4.

15. Cruciani E., Mimun H.A., Quattropani M. et al. Phase transition of the k-majority dynamics in biased communication models. *Distrib. Comput.* 2023. Vol. 36. Pp. 107-135. https://doi.org/10.1007/s00446-023-00444-2.

16. Awwama Emad, Kadi Mohammad, Krayem Said, Lazar Ivo, Rihawi Ahmad. Using formal methods in distributed system design. *MATEC Web Conf.* 125 02033. 2017. Vol. 125. Pp. 1-4. DOI: 10.1051/matecconf/201712502033.

17. Botta A., De Donato W., Persico V., Pescap A. Integration of Cloud Computing and Internet of Things: A Survey, *Future Generation Computer Systems.* 2016. Vol. 56. Pp. 684-700. https://doi.org/10.1016/j.future.2015.09.021

18. Misik S., Cela A., Bradac Z. Distributed Systems - A brief review of theory and practice, *IFAC-PapersOnLine*. 2016. Vol. 49. Issue 25. Pp. 318-323. ISSN 2405-8963. https://doi.org/10.1016/j.ifacol.2016.12.057

19. Wang W., Li D., Luo W., Kang Y., Wang L. Anthropomorphic diagnosis of runtime hidden behaviors in OpenMP multi-threaded applications, *Journal of Parallel and Distributed Computing*. 2023. Vol. 177. Pp. 17-27. ISSN 0743-7315, https://doi.org/10.1016/j.jpdc.2023.02.012.

20. Network Intrusion Detection System. URL: https://www.sciencedirect.com/topics/computer-science/network-based-intrusion-detection-system.

21. What is a Wireless Intrusion Prevention System (WIPS)? Wi-Fi Security That's No Longer Up in the Air. URL: https://www.justfirewalls.com/what-is-a-wireless-intrusion-prevention-system/.

22. Hossein Ashtari. What Is Network Behavior Analysis? Definition, Importance, and Best Practices. Network behavior analysis solutions collect and analyze enterprise network data to identify unusual activity and counter security threats. URL: https://www.spiceworks.com/tech/networking/articles/network-behavior-analysis/.

23. Lysenko S., Bobrovnikova K., Shchuka R., Savenko O. A Cyberattacks Detection Technique Based on Evolutionary Algorithms. *11th International Conference on Dependable Systems, Services and Technologies* (DESSERT). 2020. Vol. 1. Pp. 127-132. http://dx.doi.org/10.1109/DESSERT50317.2020.9125016

24. Lysenko S. Savenko O., Bobrovnikova K., Kryshchuk A., Savenko B. Information technology for detection based on their behaviour in the corporate area network. *Communications in Computer and Information Science*, ISSN: 1865–0929. 2017. Vol. 718. Pp. 166–181. https://doi.org/10.1007/978-3-319-59767-6_14

25. Murthy J.K. A Functional Decomposition of Virus and Worm Programs. In: Qing, S., Gollmann, D., Zhou, J. (eds) Information and Communications Security. ICICS 2003. *Lecture Notes in Computer Science*. Springer, Berlin, Heidelberg. 2003. Vol. 2836. Pp. 405-414. https://doi.org/10.1007/978-3-540-39927-8_37

26. Desmedt Y. Trojan Horses, Computer Viruses, and Worms. In: van Tilborg, H.C.A., Jajodia, S. (eds) *Encyclopedia of Cryptography and Security.* Springer, Boston, MA. 2011. Pp. 1319–1320. https://doi.org/10.1007/978-1-4419-5906-5_331

27. Sheikh A. Trojans, Backdoors, Viruses, and Worms. In: Certified Ethical Hacker (CEH) *Preparation Guide*. Apress, Berkeley, CA. 2021. 217 p. https://doi.org/10.1007/978-1-4842-7258-9_5

28. Shaojie W., Qiming L. Analysis of a Mathematical Model for Worm Virus Propagation. Advances in Information Security and Its Application. ISA 2009. *Communications in Computer and Information Science*. Springer, Berlin, Heidelberg. 2009. Vol. 36. Pp. 78-84. https://doi.org/10.1007/978-3-642-02633-1_10

29. Pham VH., Dacier M., Urvoy-Keller G., En-Najjary T. The Quest for Multi-headed Worms. In: Zamboni, D. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2008. *Lecture Notes in Computer Science.* Springer, Berlin, Heidelberg. 2008. Vol. 5137. Pp. 247–266. https://doi.org/10.1007/978-3-540-70542-0_13

30. Ngo F.T., Agarwal A., Govindu R., MacDonald C. Malicious Software Threats. In: *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Palgrave Macmillan, Cham. 2019. Pp. 1-22. https://doi.org/10.1007/978-3-319-90307-1_35-1

31. Edge C., Barker W., Hunter B., Sullivan G. Malware Security: Combating Viruses, Worms, and Root Kits. In: *Enterprise Mac Security*. Apress. 2010. Pp. 213–232. https://doi.org/10.1007/978-1-4302-2731-1_8

Savenko B.O. METHOD OF SYNTHESIZING MATHEMATICAL MODELS OF SECURITY LEVELS FOR PARTIALLY CENTRALIZED DISTRIBUTED MALWARE DETECTION SYSTEMS

Attackers continue to actively develop, use and distribute malicious software. The development of methods of detection and countermeasures for use in corporate networks is a particularly relevant issue in countering malicious software. Such tools should be based on new methods and take into account the features of such architectures in the processes of countering and detecting malicious software. The purpose of the work is to develop a method of synthesizing mathematical models of security levels for new types of means of detecting malicious software in corporate networks. The developed means are self-organized distributed systems with partial centralization. Partial centralization as a property of the system is defined in such a way that in order to make a decision on the further steps of the system, the set of components that contain the decision-making center of the system will be considered as a decentralized subsystem. Management of the system will be carried out by the decision-making center, which is distributed initially in the specified components and can change its location in the remaining components during its operation. To determine the states of system components, characteristic indicators are proposed and generalized analytical expressions for their calculation are developed. These characteristic indicators set the states of the components of the distributed system. The work summarizes the formation of such characteristic indicators of system components. Characteristic indicators can be continuous and discrete values, therefore, different options for their presentation and value processing have been developed for each case. A method of synthesizing mathematical models of security levels has been developed to generalize the characteristic indicators. Such calculations make it possible to assess the state of components in the system in order to independently determine its next steps. As a result, the formed system becomes the basis for filling it with malware detection methods in combination with system components as a complete sensor. To test the system, the method of detecting worm viruses was implemented in it and experiments were conducted. The results of experimental studies confirmed the effectiveness of the proposed solution.

Further research will be conducted to include additional characteristic indicators of signs and implementation in the system of malware detection methods.

Key words: *partial centralization, self-organization, malicious software, worm virus, distributed system.*