МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

БАЛАКІН СЕРГІЙ В'ЯЧЕСЛАВОВИЧ

УДК 004.056.53 (043.3)

МЕТОДИ ТА ЗАСОБИ ПІДВИЩЕННЯ ДОСТОВІРНОСТІ ІДЕНТИФІКАЦІЇ НЕСАНКЦІОНОВАНИХ ДІЙ ТА АТАК В КОМП'ЮТЕРНІЙ МЕРЕЖІ

05.13.05 – комп' ютерні системи та компоненти

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2018

Дисертацією є рукопис.

Робота виконана в Національному авіаційному університеті
Міністерства освіти і науки України.

Науковий керівник:

доктор технічних наук, професор
Жуков Ігор Анатолійович,
Національний авіаційний університет,
завідувач кафедри комп'ютерних систем та мереж.

Офіційні опоненти:

доктор технічних наук, старший науковий співробітник
Чемерис Олександр Анатолійович,
Інститут проблем моделювання в енергетиці ім. Г.Є Пухова НАН України,
заступник директора з наукової роботи;

кандидат технічних наук, старший науковий співробітник
Галелюка Ігор Богданович,
Інститут кібернетики ім. В.М. Глушкова НАН України,
провідний науковий співробітник.

Захист відбудеться «14» лютого 2019 року о 13.13 годині в ауд. 6.202 (6 корпус) на засіданні спеціалізованої вченої ради Д 26.062.07 Національного авіаційного університету за адресою: 03680, м. Київ, просп. Космонавта Комарова, 1.

З дисертацією можна ознайомитись у науково-технічній бібліотеці Національного авіаційного університету за адресою: 03680, м. Київ, просп. Космонавта Комарова, 1.

Автореферат розісланий «10» січня 2019 р.

Учений секретар
спеціалізованої вченої ради О.В. Толстікова

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Технології глобальних комп'ютерних мереж, що стрімко розвиваються, формують в інформаційній області нову систему відносин, яка відображає реалії технічного рівня сучасного людства. Інтенсивність змін значною мірою диктується тим величезним значенням, якого набуває інформація в постіндустріальному суспільстві, де вона стає головним ресурсом та інструментом одночасно.

У такому інформаційному просторі стрімко зростає кількість шкідливих програм і атак на комп'ютерні мережі, з якими в переважній більшості справляються антивіруси і фаєрволи, хоча деякі атаки можуть обійти такий захист, приносячи шкоду користувачеві або компанії. Найчастіше наявний захист спрацьовує з запізненням, коли система вже була атакована і відбулася втрата даних або контролю над певними компонентами мережі. Завдяки технічному прогресу зростає і складність способів проникнути в систему користувача.

На даному етапі більшість антивірусних компаній надають користувачеві обмежений рівень захисту, котрий не завжди вчасний (спочатку йде поширення вірусу і тільки потім антивіруси займаються його «лікуванням»), чого цілком достатньо для отримання доступу до потрібної інформації або її пошкодження. Своєчасне оповіщення користувача допомогло б підвищити ефективність виявлення несанкціонованих дій (НД) як в локальній, так і в мережі інтернет.

Дана робота описує один із варіантів недоліків захисту від несанкціонованих дій у комп'ютерні мережі, який можна впровадити в уже існуючі системи.

Аналіз літературних джерел показав, що відомі методи протидії НД обмежені й малоефективні, а також потребують постійної модернізації та оновлення для підтримки роботи з новими несанкціонованими діями. Це свідчить про те, що задача підвищення ефективності виявлення НД в комп'ютерних мережах є актуальною.

Способи та методи виявлення вторгнень в комп'ютерних мережах описуються науковцями такими, як: Я. Янг, І.В. Котенко, М. Якобссон, С. Ветзель, В.І. Городецький, Н. Репп, Р. Хекманн, Г. Вігна, К. Вішал, Р.А. Кеммерер, К. Крюгель, Р. Вегнер, А.П. Демпстер, А.А. Романюхи, Л.Н. Кастро та ін.

Не зважаючи на прогрес і численні роботи, присвячені виявленню НД в комп'ютерні мережі, треба відзначити, що вони мають особливості, які значно обмежують ефективність сучасних інструментальних засобів. Тому питання

розробки методів і моделей виявлення НД набуває актуальності. Завдання, які при цьому виникають, зумовили напрямок досліджень дисертаційної роботи.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційну роботу виконано в рамках науково-дослідницьких робіт кафедри комп' ютерних систем та мереж: НДР № 682-ДБ13 за темою «Розроблення теорії, методів та технологій оптимального управління гарантоздатною комп'ютерною мережею» (номер державної реєстрації 0113U000028), у процесі виконання якої автор дисертації брав участь у розробці методики проведення експериментальних досліджень та обробці отриманих даних; кафедральна НДР № 17/09.01.04 за темою «Системна інтеграція науково-навчального забезпечення другого рівня підготовки фахівців спеціальності 123 – комп'ютерна інженерія», у процесі виконання якої автор дисертації брав участь у реалізації методики підготовки фахівців.

Мета і задачі дослідження.

Метою роботи є забезпечення виявлення несанкціонованих дій в комп'ютерних мережах за рахунок розширення можливостей по їх обробці.

Основні задачі дослідження відповідно до поставленої мети полягають у наступному:

- проаналізувати існуючі методи і засоби розпізнавання несанкціонованих дій в комп'ютерних мережах;
- проаналізувати інструментальну базу для діагностування вторгнень у комп'ютерні мережі;
- розробити моделі виявлення несанкціонованих дій в комп'ютерних мережах на основі діагностування симптомів вторгнень;
- розробити метод діагностування вторгнень в комп'ютерні мережі за допомогою операторів теорії Демпстера-Шефера (ТДШ);
- розробити моделі аналізатора вторгнень в комп'ютерні мережі на основі даних поведінкового аналізу трафіку користувача;
- розробити метод виявлення несанкціонованих дій в комп'ютерних мережах на основі роботи елементів штучної імунної мережі;
- порівняти запропоновані методи;
- впроваджувати результати роботи на підприємствах та в навчальному процесі.

Об'єкт дослідження – розпізнавання несанкціонованих дій в комп'ютерних мережах.

Предмет дослідження – методи, системи та моделі ефективного виявлення несанкціонованих дій в комп'ютерних мережах.

Методи досліджень базуються на використанні теорії штучних імунних систем та операторів теорії Демпстера-Шафера, що дозволили синтезувати нові

методи та моделі розпізнавання НД в комп'ютерній мережі з можливістю їх реалізації, засоби евристичного аналізу забезпечили можливість навчання запропонованих моделей і налаштування їх на виявлення НД та статистичні засоби математичного оброблення результатів комп'ютерних експериментів для відбору та порівняння ефективності запропонованих методів.

Наукова новизна одержаних результатів полягає в наступному:

- удосконалено модель виявлення НД в комп'ютерній мережі, в якій розпізнавання відбувається за допомогою аналізу поведінкових ознак, що дає можливість автономно розпізнавати невідомі вторгнення і мінімізувати помилкові спрацьовування;

- отримав подальший розвиток метод виявлення вторгнень у комп'ютерні мережі, який базується на використанні операторів штучних імунних мереж для побудови структурованої мережі антитіл, що зі свого боку позитивно впливає на швидкодію і достовірність автономного виявлення як відомих, так і нових вторгнень;

- запропоновано модель виявлення вторгнень в комп'ютерній мережі засобами інспектування стану системи на виникнення аномальної поведінки, використовуючи дерево діагностування, що дозволяє відстежувати активність системи й симптомізувати дії користувача, а шляхом введення нових елементів і діапазонів роботи досягається підвищення достовірності виявлення атак;

- вперше розроблено метод розпізнавання НД засобами діагностування на основі операторів теорії Демпстера-Шафера, де на відміну від існуючих пропонується відстежувати часові фрагменти на заданих діапазонах часу і з них, за допомогою операторів злиття, формувати діагнози, за рахунок чого досягатиметься можливість автономного виявлення невідомих системі НД.

Практичне значення одержаних результатів. Розроблені в дисертаційній роботі методи та моделі можуть бути використані для підвищення виявлення НД в комп'ютерній мережі та доведені до рівня програмних засобів. Експериментальні дослідження підтверджують основні положення, що виносяться на захист. Розроблені методи підвищення ефективності виявлення НД можуть бути застосовані для забезпечення роботи засобів керування мережею, а також відповідних систем операційної підтримки. Новизну запропонованих рішень захищено патентами на корисну модель України № 110330 та № 123634.

Результати дисертаційної роботи впроваджено в навчальний процес на кафедрі комп'ютерних систем та мереж Національного авіаційного університету та використовуються в навчальних курсах: «Телекомунікаційні технології комп'ютерних мереж» і «Архітектура комп'ютерів». Результати роботи використані для підвищення ефективності діагностування

несанкціонованих дій в комп'ютерній мережі ТОВ «Газбудсервіс», а також для аналізу несанкціонованих дій в комп'ютерній мережі ДП «Короп-пласт», що підтверджено відповідними актами про впровадження.

Особистий внесок здобувача. Усі основні положення та результати дисертаційної роботи отримані автором самостійно. У роботах, виконаних у співавторстві, автору належать такі результати: у праці [2] – розроблено й обґрунтовано використання методу виявлення відхилень для ідентифікації вторгнень; [5] – виконано аналіз особливостей і вимог, які повинна задовольняти комп'ютерна мережа для можливості ідентифікації вторгнень методом усередненого часу звернення, обґрунтовано його ефективність і коректність; [6] – аналіз ефективності виявлення вторгнень на основі імунних систем; [4] – ідея використання відхилень в отриманих значеннях від усереднених для виявлення можливих вторгнень та розробка теоретичних засад для їх ідентифікації; [8] – запропоновано використання фільтрації вхідних пакетів за допомогою діапазонів активності; [9] – запропоновано механізм діагностування несанкціонованих дій в комп'ютерній мережі.

Апробація результатів роботи. Основні положення дисертаційної роботи доповідалися на XIV-й міжнародній науково-практичній конференції «Політ. Сучасні проблеми науки» (Київ, 2-3 квітня 2014 р.); на VIII міжнародній науково-технічній конференції «Комп'ютерні системи та мережні технології» (м. Київ, 16-18 квітня 2015 р.); міжнародній науково-технічній конференції «Cyber forum DESSERT 2016 B2S – S2B » (Чернівці, 18-23 травня 2016 р.); на IX міжнародній науково-технічній конференції «Комп'ютерні системи та мережні технології» (м. Київ, 21-23 квітня 2016 р.); на X-й міжнародній науково-технічній конференції «Комп'ютерні системи та мережні технології» (м. Київ, 20-22 квітня 2017 р.).

Публікації. За результатами досліджень опубліковано 14 наукових праць, у тому числі 7 статей у наукових фахових виданнях України [1-7], які включені до міжнародних наукометричних баз, 2 патенти України на корисну модель [8, 9] та 5 тез доповідей в збірниках матеріалів конференцій [10-14].

Структура та обсяг дисертаційної роботи. Дисертація складається із вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел і має 131 сторінку основного тексту, 22 рисунки, 7 таблиць, 6 сторінок додатків. Список використаних джерел містить 146 найменування і займає 14 сторінок. Загальний обсяг роботи 151 сторінка.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність роботи, визначено об’єкт і предмет дослідження, сформульовано мету і завдання, визначено наукову новизну та практичну цінність отриманих результатів.

У **першому розділі** виконано аналіз сучасних методів і засобів побудови, розвитку та виявлення НД в комп’ютерних мережах. Визначено особливості НД та їх основні складові.

Сформульовано необхідні критерії та вимоги для забезпечення своєчасного виявлення НД у комп’ютерні мережі. Визначено основні напрями розвитку сучасних методів аналізу вторгнень і можливості автономного виявлення НД. Аналіз сучасних вторгнень показав доцільність розроблення методів, котрі дадуть змогу виявляти як відомі, так і нові НД.

Проведено порівняльний аналіз моделей і методів, які можливо використовувати при розпізнаванні НД в комп’ютерній мережі. Порівняно характеристики методів і вказано на їх сильні та слабкі сторони. Сформовано вимоги до вибраних методів на основі збереження швидкодії та можливості автономного виявлення НД (без використання і звернення до сигнатурних баз даних). Розглянуто методи штучних імунних систем, котрі дають змогу підтримувати автономне виявлення нових НД при високій швидкості обробки інформації та адаптивності. Виявлення НД за допомогою діагностування дає можливість розширити спектр потенціальних вторгнень за допомогою використання операторів ТДШ. При поєднанні різних технологій при використанні методів ТДШ можливо досягнути високої швидкості та надійності виявлення НД в комп’ютерних мережах.

Описано основні недоліки та обмеження розглянутих інструментів. Сформовано основні задачі дослідження, визначені шляхи виявлення несанкціонованих дій у комп’ютерні мережі засобами ШІМ і ДТШ. Визначено основні напрямки та сформовані основні завдання дисертаційного дослідження.

У **другому розділі** на основі ШІМ запропоновано використання евристичного аналізатора НД, в якому робота антигенів і антитіл відповідатиме вхідним даним та необхідним рішенням задач відповідно. Схема аналізатора показана на рис.1

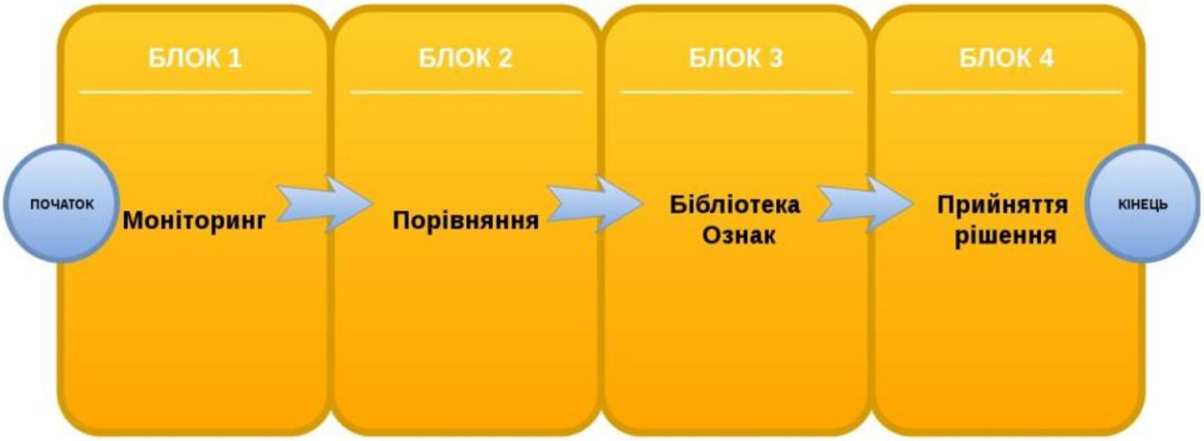

Рис. 1. Модель аналізатора несанкціонованих дій

Обґрунтовується застосування такої схеми аналізатора тим, що кожний блок виконуватиме конкретну логічну функцію. Моніторинг дозволить отримати протоколи НД та звичайних дій користувача. Порівняння протоколів дій вторгнень і користувача дозволить отримати інформацію про наявність в них спільних ознак. За збереження виявлених у попередньому кроці ознак відповідатиме блок бібліотеки ознак (він також фіксуватиме частоту їх появи для присвоєння відповідного рейтингу). Останній блок буде відповідати за належність даної дії до несанкціонованих.

Обґрунтовується застосування бібліотек поведінки, за допомогою яких пропонується відстежувати зміни в системі. На основі отриманих даних про поведінку таких дій в НД будуть складатися ознаки вторгнень.

Проаналізовано моделі ШІМ, на основі яких можливо побудувати вищеописаний аналізатор. Вибрано ШІМ, котра опрацьовує НД за допомогою антитіл. ШІМ автономно виявляє вторгнення без використання готових сигнатур НД без зменшення загальної швидкодії системи. Узагальнено ШІМ зведена до наступного виду:

$$\mathrm{AIS} = (\mathrm{G}, \mathrm{A}, \mathrm{c}, \mathrm{S}) = [\mathrm{Int}(\mathrm{G}, \mathrm{A}) \rightarrow \mathrm{Rate}(\mathrm{A}) \rightarrow \mathrm{Ext}(\mathrm{A}) \rightarrow$$
$$\rightarrow \mathrm{Mut}(\mathrm{cl}, \mathrm{G}) \rightarrow \mathrm{Membest}(\mathrm{cl}) \rightarrow \mathrm{Del}(\mathrm{A}, \mathrm{cl}, \mathrm{c})] \rightarrow \mathrm{End}(\mathrm{S}),$$

де G –антигени;

A –антитіла;

c – межа близькості;

S – умова закінчення.

Приведена AIS виконується операторами:

Int(G,A) – представлення антитіл A антигенам G, через обчислення їх подібностей (F):

$$F_{A-G} = (1 - d_{A-G})^{-1},$$

де d_{A-G} – відстань між антитілом A та антигенами G;

$\mathrm{Rate(A)}$ –відбір антитіл з найвищою подібністю;

$\mathrm{Ext(A)}$ – розширення популяції відібраних антитіл шляхом клонування їх зразків з найвищою подібністю;

$\mathrm{Mut(G, cl)}$ – мутація клонів cl і антигенів G ;

$\mathrm{Membest(Cl)}$ – утворення пам'яті клонів з найвищою подібністю;

$\mathrm{Del(\ A, cl, c)}$ – видалення A і cl в яких подібність вища межі близькості c;

$\mathrm{End(S)}$ – кінець циклу при досягненні умови закінчення S.

Для виявлення НД підійдуть методи клонального відбору та мережевої взаємодії.

За допомогою введення нових змінних пришвидшено процеси клонування і мутації антитіл. Описано вплив на імунні механізми клонування. Повільність такої ШІМ пояснюється затратами часу на обчислення нових поколінь при клонуванні. Для своєчасного виявлення НД потрібно регулювати клонування введенням меж кратності:

$$N_c(A) = \begin{cases} N_{c\_min} \text{ при } F(A) \leq F_{best} * 0.35, \\ N_{c\_max} \text{ при } F(A) \geq F_{best} * 0.65, \\ F(A)\ \dfrac{F(A) - F_{best} * 0.25}{F_{best} * 0.4}, \end{cases}$$

де N_{c_min} і N_{c_max} – межі кратності;

$F(A)$ – подібність антитіла A;

F_{best} – найкраща подібність всього покоління.

Також важливо провести мутацію антитіл в ШІМ, котра задає ймовірність і крок процесу мутації:

$$P_m(A) = P_{mmax} * \frac{(F(A) - F_{best})}{(F_{worst} - F_{best})} + \frac{(F_{best} - F(A))}{(F_{worst} - F_{best})} * P_{mmin},$$

де P_{mmin} и P_{mmax} – відображають граничну ймовірність мутації антитіла.

Крок мутації корелюється в залежності від значення подібності антитіл з виборки автоматично (при високій подібності – крок мутації зменшується, і навпаки).

Проаналізовано інструменти та оператори ШІМ, застосовуючи котрі можна реалізувати запропонований аналізатор з рис.1. У режимі виявлення НД даний аналізатор опрацьовує вторгнення для отримання їх протоколів. Порівнюючи протоколи НД, отримаємо інформацію про наявність в них спільних ознак. Далі для цих ознак вираховуються рейтинги появи (необхідні для ведення статистики однорідних елементів). Після вирахування рейтингів

для усіх НД починається процес навчання ШІМ. Навчання базується на основі рейтингів появи НД, що дає можливість програмувати антитіла на виявлення антигенів (як вторгнень, так і звичайної активності користувача).

Після закінчення навчання починається виявлення НД. Для виявлення НД в досліджуваних протоколах проводиться пошук фрагментів вторгнень з бібліотеки ознак (котра зберігає рейтинги). Знайдені рейтинги посилаються в навчену ШІМ для віднесення дій до НД чи звичайної роботи системи.

Для виявлення невідомих НД необхідно провести аналогічний аналіз дій користувача (дій, що не підпадають по опису до НД). Для цього виконуються аналогічні дії що і для НД, але в протоколах отриманих дій користувача проводимо пошук фрагментів НД (котрі були збережені в блоці бібліотеки ознак). Для навчання ШІМ використовуються рейтинги НД для звичайних дій в системі. При навчанні ШІС вхідні дані будуть відноситись до НД чи звичайних дій в системі (або невідомих НД). Після процесу навчання ШІМ являтиме собою множину антитіл пам'яті антитіл (відображуватиме антигени мережі) та матрицю їх подібностей B (відображуватиме зв'язки антитіл). Значення подібностей дають змогу виявити антитіла, що розпізнаватимуть антигени як НД, так і звичайних дій с системі (чи вторгнень невідомого типу).

Запропоновано й обґрунтовано доцільність використання даного підходу. Розглянуто принципи ШІМ для організації виявлення НД. Сформульовано недоліки сучасних систем виявлення НД у порівнянні з приведеними методами.

У **третьому розділі** запропоновано за допомогою віртуальної інструментальної бази Deterlab реалізувати діагностування НД за допомогою операторів ТДШ, котрі будуть використовуватися при діагностуванні для контролю часових фрагментів і формування даних для визначення симптомів і сигнатур вторгнень. Для вирішення задачі розпізнавання НД методом діагностування використано принципи роботи операторів ТДШ. Запропоновано використати наступну модель виявлення вторгнень (рис. 2):

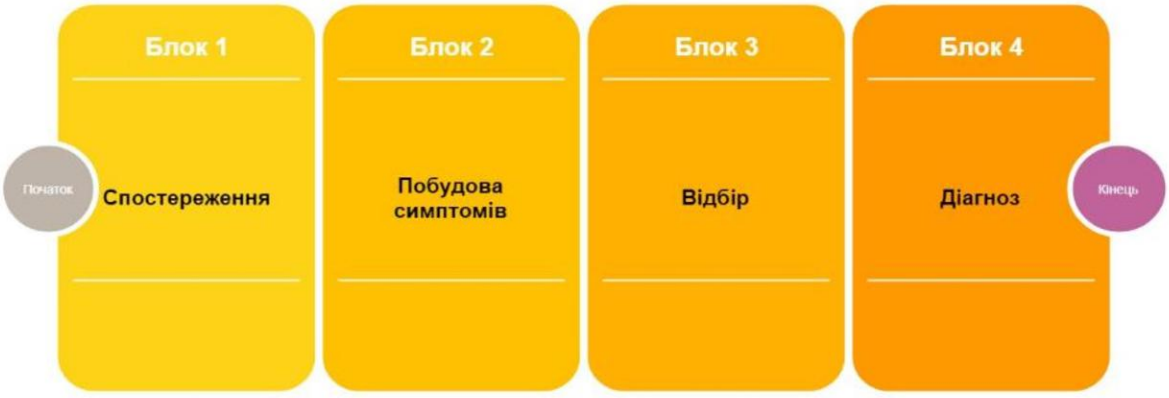

Рис. 2. Модель діагностування несанкціонованих дій

Обґрунтовано використання операторів ТДШ для організації процесу діагностування і виявлення НД. На основі спостережень і зібраних доказів будуються симптоми, котрі після процесу відбору дають можливість відносити певні типи активностей в мережі до вторгнень чи звичайних дій системи.

В результаті експерименту було перевірено достовірність і можливості діагностування при виявленні атак і несанкціонованих дій. Експеримент проводився на базі інструментальної системи DeterLab, що дає змогу реалізувати всі компоненти розробленого методу і провести їх тестування. Один із вузлів був налаштований на роботу з трафіком, інші два – на роботу з атаками на систему. Саме дослідження відбувалось при одночасному, або комбінованому запуску всіх вузлів, для того, щоб система могла діагностувати наявність НД.

Узагальнено процес діагностування зведено до наступного виду:

$$DTR = (Obs, Symp, Sel) = [Present\ (Obs) \rightarrow Check(Symp) \rightarrow Sel(Symp) \rightarrow Get\ (SymptA, SymptP)] \rightarrow Diagn,$$

де, Obs – відбір ознак спостережуваних;

$Symp$ – симптоми;

Sel – критерій відбору.

При роботі виконуються наступні оператори:

Present (Obs) – оператор представлення спостережуваних (O), котрий має можливість відношення до часових фрагментів шляхом запису значення цього параметра стану в кожен момент часу;

Check (Symp) – перевірка спостережуваних на наявність в них симптомів, які будуть служити для діагностики стану S. Якщо спостережувана не є актуальною, вона не сприятиме діагностиці стану S і не буде включена в набір спостережуваних O;

Sel (Symp) – відбір ознак симптомів (st) з набору спостережуваних. Пов'язані з кожним симптомом спостережувані визначаються функцією STO, яка приймає симптом і повертає відповідне значення спостереження на виході. Значення симптому st в момент часу t, визначається через st(STO(st)(t)), припускаючи, що st раніше міг вже використовуватись;

Get (SymptA, SymptP) – після операції відбору отримуємо на виході інформацію про наявність симптому (SymptP), чи його відсутність (SymptA);

Diagn – винесення діагнозу на основі сукупності отриманих симптомів з набору спостережуваних. Мета діагностування – визначити повністю спостережувану систему S і дерево діагностики DT, яке класифікує стани S для визначення ефективності діагнозу. Таким чином, за допомогою DT системи (s),

в будь-який момент часу t, вираженому через $DT_S(S,t)$, стає можливим отримання діагнозу S. В даному випадку $DT_S(S,t)$ буде рішенням поставленої задачі. Якщо $DT_S(S,t)$ повертає значення, відмінне від всієї сукупності вершини DT_g, то відомо, що система нині поводиться нормально, тобто $DT_S(S,t)$ повертає вершину нормальності. Якщо система поводиться аномально, то $DT_S(S,t)$ повертає вершину аномалії. Діагностування працює як класичний детектор аномалій, інформуючи, коли S перестає працювати в звичайному режимі.

Інспектування стану системи на виникнення аномальної активності, використовуючи дерево діагностування, дає змогу моніторити активність системи користувача. Діагностування проводиться в режимі реального часу і дозволяє вчасно реагувати на порушення. Як вхідні характеристики для діагностування беруться дані про роботу системи на рівних проміжках часу. З цих даних генеруються звіти про відмінності від еталонних значень в системі і формуються повідомлення про несанкціоновані дії або підозрілу активність. При нормальній роботі система продовжує функціонувати в звичайному режимі.

Досліджено можливість застосування операторів ТДШ для опису даної моделі опрацювання симптомів вторгнень. Удосконалено механізми обробки спостережуваних для мінімізації отримання хибних діагнозів. Описано роботу алгоритму виявлення змін (csm) відповідним рівнянням:

$$\text{csm(T, ul, } \mu, \sigma, \text{ a)(i)} = \begin{cases} 1 & \text{S}_\text{i} \geq \text{a} \ \wedge \ \text{ul} = 1 \\ 0 & \text{S}_\text{i} < \text{a} \ \wedge \ \text{ul} = 1 \\ 1 & \text{S}_\text{i} \leq -\text{a} \ \wedge \ \text{ul} = 0\text{'} \\ 0 & \text{S}_\text{i} > -\text{a} \ \wedge \ \text{ul} = 0 \end{cases}$$

$$\text{csm}(\text{T}, \text{ul}, \mu, \sigma, \text{a})_t(i) = \ \text{T}_t(i),$$

де, T - функція вводу часових фрагментів, ul – верхній/нижній селектор виявлення зміни, μ – середнє відхилення, σ – стандартне відхилення, a – поріг тривоги. За рахунок введення порогового алгоритму виявлення змін досягається підвищення достовірності виявлення НД.

Запропоновано додатково використовувати алгоритми затримки, котрі дають можливість зменшити кількість продукованих системою симптомів, мінімізуючи при цьому витрати на час постановки кінцевого діагнозу. Запропонована структура дерева діагностування для роботи з несанкціонованими діями. Описано використання часових фрагментів і часових рядів. У рамках ТДШ діагноз вторгнень формується через введення поняття «основне переконання» (ОП), а опис станів системи забезпечується структурою проникливості SRT, яка визначається масивом SRT = {SRT_1, SRT_2 , … , SRT_i}, де

для $1 \leq i \leq N$, SRT_i визначає конкретний стан системи. Так само ОП є функцією f_{srt}, де SRT являє собою пов'язану структуру проникнення. f_{srt} відображає будь-яку підмножину структури проникнення для реального значення, f_{srt}: P(SRT) → R. Значення в діапазоні позначається як маса переконання. Для позначення меж роботи ОП використовуються нижня і верхня ймовірність:

$$pl(f_{srt}, A) = 1 - bl(f_{srt}, SRT/A),$$

де $bl(f_{srt}, A) = \sum_{B \subseteq A} f_{srt}(B)$ – нижня межа суб'єктивної ймовірності (переконання); $pl(f_{srt}, A) = \sum_{B \cap A \neq \emptyset} f_{srt}(B)$ – верхня межа суб'єктивної ймовірності (правдоподібність); A – набір станів.

Далі, для компонування декількох різних ОП в одну використовуються оператори злиття, які описуються рівнянням:

$$n(SRT, A_{srt}, B_{srt}) = \sum_{x,y \in P(SRT) | x \cap y = 0} A_{srt}(x) B_{srt}(y).$$

Вхідні ОП (A_{srt}, B_{srt}) знаходяться в одній SRT. Допоміжна функція n (коли задані два ОП однієї структури проникливості) обчислює загальну кількість мас в суперечливих одна одній частинах доказів (коли множини переходів не мають загальних станів) A_{srt} і B_{srt}. Незалежні групи об'єднуються незалежними операторами злиття.

Дано визначення системи й станів, в яких перебуває система, а також вимоги до цих станів. Для забезпечення функціонування та організації станів системи на різних рівнях деталізації ведено дерево специфікацій. Воно використовується для побудови дерева діагностики, котре моделює аномальну поведінку системи. Дано пояснення спостережуваності й того, як формуються і використовуються симптоми для діагностики системи. Показано, як кілька симптомів можуть бути об'єднані разом для постановки діагнозу. Введено функції налаштування маси симптомів для підвищення достовірності розрахунків.

Симптоми формуються на основі внутрішніх станів, котрі можуть використовуватися кілька разів, що може привести до різних ОП на виході. Симптоми отримують дані від спостережуваних як тільки вони стають доступними.

Основою процесу діагностування є дерево специфікацій, що використовується для представлення всіх діагнозів, в яких може перебувати система (S). Першим кроком моделювання дерева діагностики в ТДШ буде пов'язання всіх станів системи з конкретним ідентифікатором. Формується

набір станів SSn з простору ідентифікаторів SS = $\{ns, as_0, as_1, \dots, as_{A_{n-1}}\}$ (SS означає «простір станів»). Ідентифікатор простору станів ns $\in$ SS відповідає всім станам, пов'язаним з вершиною нормальності дерева діагностики (ns означає «нормальний стан»). Ідентифікатори простору станів $\{\{as_0, as_1, \dots, as_{A_{n-1}}\} \in$ SS (as означає «стан атак»), відповідають станам атаки A = $\{a_0, a_1, \dots, a_{A_{n-1}}\}$. Утворюється простір станів SS, що являє собою структуру проникнення в ТДШ.

Для постановки діагнозу стану S потрібно мати цілісну ОП. Необхідно поєднати набори ОП для формування єдиної ОП, котра буде відображати їхню суть. Поєднання ОП проводиться операторами злиття. Якщо всі симптоми приймаються як незалежні один від одного (тобто лежать в основі спостереження), то кожна змінна відстежується окремо і об'єднується незалежними операторами злиття. Якщо симптоми залежні, то один оператор злиття може об'єднувати всі ОП. Якщо групи симптомів будуть залежати один від одного, то необхідно буде використовувати два оператори злиття. Виходить, що один залежний оператор злиття буде об'єднувати всі залежні групи ОП в одну незалежну. Це дасть змогу сформувати набір незалежних основ переконань, що будуть еквівалентні за розміром до числа залежних груп. Надалі незалежні ОП утворять кінцеву ОП, яка являтиме собою дані, отримані кожним із симптомів в S, які описуватимуть стани DT системи в моменті часу t. Стане можливою оцінка поточного стану системи в будь-який момент часу t DT_S (S,t).

На заключному етапі визначається, чи знаходиться S в стані конкретної атаки з масиву пов'язаних класів атак a∈ac. Кожна атака буде містити елемент з масиву атак {a} ⊂ A. Обчислюється ймовірність стану для кожної атаки: bl(B_{DT_f}, {a}), pl(B_{DT_f}, {a}), ∀{a} ∈ ac. Якщо атака не відповідає жодному ідентифікатору, то система знаходиться в стані невідомого вторгнення. Якщо виявлена вершина атаки, то вибирається атака з найбільшою суб'єктивною ймовірністю і процес діагностики закінчується.

Сформульовано вимоги до несанкціонованих дій у системі та описано методи їх виявлення та обробки. Розглянуто вирішення завдань, пов'язаних з організацією виявлення вторгнень шляхом діагностування за допомогою використання інструментів ТДШ, що забезпечують оптимальний розподіл ресурсів системи та гарантують виявлення невідомих системі вторгнень, що не входили до набору наперед заданих НД.

В четвертому розділі розглянуто питання реалізації інструментальних засобів та проведена експериментальна перевірка досліджень. Проведено вибір інструментів для реалізації моделювання і впровадження запропонованих методів з метою підвищення виявлення НД в комп'ютерних мережах.

При реалізації методів підвищення виявлення НД за допомогою ШІМ використані можливості стандартного емулятора Demulate, котрий дає можливість створити штучне середовище для проведення досліджень. На базі емулятора проведено моніторинг за системними викликами та основні розрахунки по виявленню несанкціонованих дій в комп'ютерній мережі.

Проведено дослідження ефективності методу виявлення НД в комп'ютерній мережі на основі штучних імунних систем і діагностування. На основі аналізу отриманої інформації зроблений наступний висновок: при коректній навчальній вибірці та вірному виборі параметрів навчання метод ШІМ має однаково високу достовірність виявлення нових НД як і метод діагностування. ШІМ потребує додаткового часу на утворення навчальної вибірки, але це дозволяє системі швидше реагувати на нові види НД і знизити кількість помилкових спрацювань. Метод діагностування менше навантажує систему користувача, але частіше визначає підозрілу активність як НД.

Виконано аналіз ефективності розпізнавання НД в порівнянні з відомими методами, обрані програмні рішення Kaspersky та AVIRA, які не змогли визначити 4 і 3 НД відповідно, що свідчить про недосконаліть даних програмних рішень при роботі з поведінковим аналізом вторгнень. Ефективність при роботі з навчальною вибіркою комплексів AVIRA і Kaspersky становить 80% і 73,3%, а запропонованих рішень – 100%. Тобто випробувані методи виявлення несанкціонованих дій в комп'ютерній мережі перевершують існуючі на 20% і 26,6% відповідно. Результати порівняльного аналізу НД показують, що запропоновані методи перевершують відомі антивірусні продукти, використані в порівняльному тесті та здатні виявити невідомі НД.

ВИСНОВКИ

У дисертаційній роботі вирішено актуальне науково-технічне завдання підвищення ефективності виявлення несанкціонованих дій в комп'ютерних мережах за рахунок використання методів ШІМ та діагностування.

Основні наукові та практичні результати дисертаційної роботи:

1. Виконано системний аналіз принципів й особливостей функціонування засобів виявлення НД в мережах, який дав підстави аргументувати доцільність і можливість створення методів виявлення несанкціонованих дій в комп'ютерних мережах;

2. Проведений огляд існуючих засобів виявлення НД в мережах дозволив визначити основні напрямки дослідження і слабкі сторони сучасних програмних рішень. Подано опис розроблюваних методів виявлення

несанкціонованих дій в комп'ютерних мережах, котрі зможуть вчасно і коректно реагувати на вторгнення і працюватимуть автономно;

3. Запропоновано модель виявлення НД в комп'ютерній мережі, в якій розпізнавання вторгнень відбувається через аналіз поведінкових ознак, що дає можливість автономно розпізнавати НД і уникати хибних спрацювань;

4. Отримав подальший розвиток метод виявлення НД в комп'ютерній мережі, який базується на використанні операторів ШІМ для побудови структурованої мережі антитіл. Отже, побудована ШІМ здатна швидше ідентифікувати як відомі, так і нові НД;

5. Представлено модель виявлення НД в комп'ютерній мережі засобами інспектування стану системи на виникнення аномальної поведінки, використовуючи дерево діагностування, що дає змогу відстежувати активність системи та симптомізувати дії користувача, а за рахунок введення нових елементів і діапазонів роботи досягається підвищення достовірності виявлення НД і мінімізація помилкових спрацювань;

6. Запропоновано метод розпізнавання НД в комп'ютерній мережі засобами діагностування на основі операторів ТДШ, де на відміну від існуючих пропонується відстежувати часові фрагменти на заданих діапазонах часу і з них, за допомогою операторів злиття, формувати діагнози. Все це дозволить автономно виявляти невідомі системі НД;

7. Проведено порівняльний аналіз запропонованих рішень, котрий експериментально підтвердив, що дані методи підвищують достовірність ідентифікації НД і атак в комп'ютерній мережі;

8. Розроблені методи та моделі використані для діагностування НД в комп'ютерній мережі ТОВ «Газбудсервіс», а також для аналізу НД в комп'ютерній мережі ДП «Короп-пласт».

Отримані результати дисертаційної роботи також впроваджено в навчальний процес на кафедрі комп'ютерних систем та мереж Національного авіаційного університету.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Балакин С. В. Выявление компьютерных атак с помощью мониторинга сетевых объектов. *Технологический аудит и резервы производства*. Харьков, 2015. № 5-6(25). С.36-38. (Входить до міжнародних наукометричних баз Index Copernicus, РИНЦ, EBSCO Publishing, DOAJ).

2. Zhukov I. A., Balakin S.V. Detection of computer attacks using outliner. *Науковий журнал «Молодий вчений»*. К.: 2016. № 9(36). С. 91-93. (Входить до

міжнародних наукометричних баз РИНЦ, ScholarGoogle, OAJI, CiteFactor, Research Bible, Index Copernicus).

3. Балакин С. В. Организация пресечения вторжений в компьютерные сети алгоритмами выявления изменений. *Вісник НТУ «ХПІ». Серія: Механіко-технологічні системи та комплекси.* Харків, 2017. № 20(1242). С.3-7. (Входить до міжнародної наукометричної бази OAJI).

4. Жуков И. А., Балакин С. В. Обнаружение компьютерних атак с помощью метода отклонений. *Радіоелектронні і комп'ютерні системи: наук. – техн. жур.* Харків, 2016. №5(79). С. 33-37. (Реферується наукометричними базами ВАК, Index Copernicus, INSPEC IDEAS).

5. Жуков И. А., Балакин С. В. Идентификация атак в компьютерной сети методом усредненного времени обращений. *Проблеми інформатизації та управління: зб. наук. праць.* К.: НАУ, 2015. № 2(50). С.65–69. (Реферується наукометричною базою Україніка наукова, входить до міжнародних наукометричних баз РИНЦ, ScholarGoogle).

6. Балакін С. В. Застосування штучних імунних систем при виявленні шкідливих программ в комп'ютерній мережі. *Проблеми інформатизації та управління: зб. наук. праць.* К.: НАУ, 2017. № 1-2(57-58). С. 61-68. (Реферується наукометричною базою Україніка наукова, входить до міжнародних наукометричних баз РИНЦ, ScholarGoogle).

7. Жуков И. А., Балакин С. В. Исследование эффективности метода обнаружения вторжений в компьютерные сети на основе искусственных иммуных систем. *Проблеми інформатизації та управління: зб. наук. праць.* К.: НАУ, 2017. № 3(59). С. 65-69. (Реферується наукометричною базою Україніка наукова, входить до міжнародних наукометричних баз РИНЦ, ScholarGoogle).

8. Спосіб запобігання комп'ютерним атакам у мережі за допомогою фільтрації вхідних пакетів: пат. 110330 Україна: МПК G06F 12/14. №201602196; заявл. 09.03.16; опубл. 10.10.16, Бюл. №19. 4 с.

9. Спосіб діагностування несанкціонованих дій в комп'ютерній мережі: пат. 123634 Україна: МПК G06F 12/14. №201702719; заявл. 23.03.17; опубл. 12.03.18, Бюл. №5. 4 с.

10. Балакин С. В. Методы и средства повишения достоверности идентификации несанкционированных воздействий и атак в компьютерной сети. *Комп'ютерні системи та мережні технології* : зб. тез доп. VIII міжнар. наук.-техн. конф., м. Київ, 16-18 квіт. 2015 р. Київ, 2015. С. 11-12.

11. Балакин С. В. Системы предотвращения атак в компьютерной сети на основе сигнатурных методов. *Комп'ютерні системи та мережні технології* : зб. тез доп. IX міжнар. наук.-техн. конф., м. Київ, 21-23 квіт. 2016 р. Київ, 2016. С. 12-13.

12. Балакин С. В. Средства диагностирования несанкционированных воздействий и атак в компьютерной сети. *Комп'ютерні системи та мережні технології* : зб. тез доп. X міжнар. наук.-техн. конф., м. Київ, 20-22 квіт. 2016 р. Київ, 2017. С. 13-14.

13. Balakin S. V. Traffic analysis for intrusion detection systems in telecommunication networks. *Політ. Сучасні проблеми науки :* зб. тез доп. XIV міжнар. наук.-практ. конф., м. Київ, 2-3 квіт. 2014. С. 59-60.

14. Балакин С. В. Оптимизация искусственных иммунных систем при идентификации несанкционированных сетевых воздействий. *Комп'ютерні системи та мережні технології :* зб. тез доп. XI міжнар. наук.-техн. конф., м. Київ, 19-21 квіт. 2018 р. Київ, 2018. С. 7-8.

АНОТАЦІЯ

Балакін С. В. Методи та засоби підвищення достовірності ідентифікації несанкціонованих дій та атак в комп'ютерній мережі. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти. – Національний авіаційний університет, МОН України, Київ, 2018.

Дисертаційну роботу присвячено вирішенню актуального науково-технічного завдання – підвищенню достовірності ідентифікації несанкціонованих дій і атак в комп'ютерній мережі.

Для ефективної, надійної та високошвидкісної ідентифікації несанкціонованих дій і атак в комп'ютерній мережі потрібно впроваджувати і використовувати методи, основані як на штучних імунних системах, так і на можливості діагностування вторгнень. Такий підхід дозволить підвищити ефективність ідентифікації несанкціонованих дій і дасть можливість автономно виявляти підозрілу активність.

У роботі визначено методи виявлення несанкціонованих дій і атак в комп'ютерній мережі за рахунок використання засобів штучних імунних систем та діагностування на основі теорії Демпстера-Шафера, котрі дають можливості ефективно протидіяти вторгненням. Досліджено можливості використання операторів імунних систем для моделювання роботи запропонованих методів. На основі цих властивостей запропоновано процедури ідентифікації несанкціонованих дій і атак в комп'ютерній мережі.

Сформульовано необхідні критерії та вимоги для забезпечення своєчасного виявлення вторгнень у комп'ютерні мережі. Визначено основні

напрями розвитку сучасних методів аналізу вторгнень і можливості автономного виявлення НД. Аналіз сучасних вторгнень показав доцільність розроблення методів, котрі дадуть змогу виявляти як відомі, так і нові НД.

Проведено порівняльний аналіз моделей і методів, які можливо використовувати при розпізнаванні НД в комп'ютерній мережі. Порівняно характеристики методів і вказано на їх сильні та слабкі сторони. Сформовано вимоги до вибраних методів на основі збереження швидкодії та можливості автономного виявлення НД (без використання і звернення до сигнатурних баз даних). Розглянуто методи штучних імунних систем, котрі дають змогу підтримувати автономне виявлення нових НД при високій швидкості обробки інформації та адаптивності. Виявлення НД за допомогою діагностування дає можливість розширити спектр потенціальних вторгнень за допомогою використання операторів ТДШ. При поєднанні різних технологій при використанні методів ТДШ можливо досягнути високої швидкості та надійності виявлення НД в комп'ютерних мережах.

Проведено дослідження ефективності методу виявлення НД в комп'ютерній мережі на основі штучних імунних систем і діагностування. На основі аналізу отриманої інформації зроблений наступний висновок: при коректній навчальній вибірці та вірному виборі параметрів навчання метод ШІМ має однаково високу достовірність виявлення нових НД як і метод діагностування. ШІМ потребує додаткового часу на утворення навчальної вибірки, але це дозволяє системі швидше реагувати на нові види НД і знизити кількість помилкових спрацювань. Метод діагностування менше навантажує систему користувача, але частіше визначає підозрілу активність як НД. Результати порівняльного аналізу НД показують, що запропоновані методи перевершують відомі антивірусні продукти, використані в порівняльному тесті та здатні виявити невідомі НД.

Теоретично та експериментально доведено ефективність запропонованих методів. Результати теоретичних та експериментальних досліджень упроваджено у виробництво та навчальний процес.

Ключові слова: комп'ютерна мережа, трафік, несанкціоновані дії, виявлення вторгнень, діагностування, штучна імунна система, ідентифікація.

АННОТАЦИЯ

Балакин С.В. Методы и средства повышения достоверности идентификации несанкционированных действий и атак в компьютерной сети. – На правах рукописи.

Диссертационная работа на соискание научной степени кандидата технических наук по специальности 05.13.05 – компьютерные системы и компоненты. – Национальный авиационный университет, МОН Украины, Киев, 2018.

Диссертационная работа посвящена решению актуальной научно-технической задачи: повышению достоверности идентификации несанкционированных действий и атак в компьютерной сети.

Для эффективной, надежной и высокоскоростной идентификации несанкционированных действий и атак в компьютерной сети нужно внедрять и использовать методы основаны как на искусственных иммунных системах, так и на возможности диагностирования вторжений. Такой подход позволит повысить эффективность идентификации несанкционированных действий и даст возможность автономно обнаруживать подозрительную активность.

В работе определены методы выявления несанкционированных действий и атак в компьютерной сети за счет использования средств искусственных иммунных систем и диагностирования на основе теории Демпстера-Шафера, которые дают возможность эффективно противодействовать вторжениям. Исследованы возможности использования операторов иммунных систем для моделирования работы предложенных методов. На основе этих свойств предложены процедуры идентификации несанкционированных действий и атак в компьютерной сети.

Теоретически и экспериментально доказана эффективность предложенных методов. Результаты теоретических и экспериментальных исследований внедрены в производство и учебный процесс.

Ключевые слова: компьютерная сеть, трафик, несанкционированные действия, обнаружение вторжений, диагностирование, искусственная иммунная система, идентификация.

ANNOTATION

Balakin S. Methods and ways of increasing the reliability of the identification of unauthorized actions and attacks in the computer network. – Manuscript.

Master's thesis initiated to get degree a candidate of technical science on speciality 05.13.05 – computer systems and components. – National Aviation University, MES of Ukraine, Kiev, 2018.

The thesis is devoted to solving the actual scientific and technical problem - increasing the reliability of identification of unauthorized actions and attacks in the computer network.

For effective, reliable and high-speed identification of unauthorized actions and attacks in a computer network, methods should be implemented and used based on both artificial immune systems and the ability to diagnose intrusions. Such an approach will increase the effectiveness of identifying unauthorized actions and will provide an opportunity to autonomously detect suspicious activity.

The work defines methods for detecting unauthorized actions and attacks in a computer network through the use of artificial immune systems and diagnostics based on the Dempster-Shafer theory, which makes it possible to effectively detect intrusions. The possibilities of using the operators of immune systems for modeling the work of the proposed methods are explored. Based on these properties, procedures are proposed for identifying unauthorized actions and attacks in a computer network.

The necessary criteria and requirements are formulated for ensuring timely detection of intrusions in computer networks. The basic directions of development of modern methods of analysis of intrusions and possibilities of autonomous detection of intrusions are determined. An analysis of modern intrusions has shown the feasibility of developing methods that will be able to detect both known and new intrusions.

A comparative analysis of models and methods that can be used for intrusion recognition in a computer network is carried out. The comparative characteristics of the methods are indicated on their strengths and weaknesses. The requirements for the selected methods are formed on the basis of maintaining the speed and the ability to independently identify the intrusion (without the use and access to signature databases). Detection of intrusions by means of diagnostics enables to expand the spectrum of potential intrusions by using Dempster-Shafer operators. When combining different technologies with the use of Dempster-Shafer methods it is possible to achieve high speed and reliability of detection of intrusions in computer networks.

The research of the effectiveness of the method of detection of intrusions in a computer network on the basis of AIS and diagnostics was carried out. On the basis of the analysis of the information obtained, the following conclusion was made: with a correct training sample and a correct choice of learning parameters, the AIS method has the same high reliability as the diagnostic method. AIS requires additional time to create a training sample, but this allows the system to respond more quickly to new types of intrusions and reduce the number of false positives. The diagnostic method is less burdensome for the user system, but more often it identifies suspicious activity as

intrusion. The results of the comparative analysis of intrusions show that the proposed methods outperform the known antiviral products used in the comparative test and are capable of detecting unknown intrusions.

Proved the effectiveness of proposed methods. The results of theoretical and experimental research are introduced into the production and educational process.

Keywords: computer network, traffic, unauthorized actions, intrusion detection, diagnosis, artificial immune system, identification.