МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

КУШНАРЬОВ МАКСИМ ВОЛОДИМИРОВИЧ

УДК 004.89

МЕТОДИ ТА МОДЕЛІ РОЗПІЗНАВАННЯ ШКІДЛИВИХ ПРОГРАМ НА ОСНОВІ ШТУЧНИХ ІМУННИХ СИСТЕМ

05.13.23 – системи та засоби штучного інтелекту

АВТОРЕФЕРАТ

дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2016

Дисертацією є рукопис.

Робота виконана у Харківському національному університеті радіоелектроніки, Міністерство освіти і науки України.

Науковий керівник – доктор технічних наук, професор
Корабльов Микола Михайлович,
Харківський національний університет радіоелектроніки, професор кафедри електронних обчислювальних машин.

Офіційні опоненти: доктор технічних наук, професор
Гороховатський Володимир Олексійович,
Харківський навчально-науковий інститут ДВНЗ «Університет банківської справи», професор кафедри інформаційних технологій

доктор технічних наук, професор
Литвиненко Володимир Іванович,
Херсонський національний технічний університет, завідувач кафедри інформатики та комп'ютерних наук

Захист відбудеться «____» _____ 2016 р. о _____ годині на засіданні спеціалізованої вченої ради Д 64.052.01 у Харківському національному університеті радіоелектроніки за адресою: 61166, м. Харків, просп. Науки, 14.

З дисертацією можна ознайомитися в бібліотеці Харківського національного університету радіоелектроніки за адресою: 61166, м. Харків, просп. Науки, 14.

Автореферат розіслано «____» _____ 2016 р.

Учений секретар
спеціалізованої вченої ради О.А. Винокурова

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Сучасні дослідження в галузі розробки систем комп'ютерної безпеки, пов'язані з необхідністю розпізнавання різноманітного шкідливого програмного забезпечення (ПЗ) та запобігання вторгнень у комп'ютер, свідчать про доцільність застосування в таких системах методів та моделей інтелектуальної обробки інформації (ІОІ), серед яких останнім часом найбільше розповсюдження отримали штучні нейронні мережі (ШНМ), штучні імунні системі (ШІС), мультиагентні системи (МАС) тощо.

Антивірусні продукти, що існують, не можуть забезпечити абсолютно надійний захист комп'ютера, що, передусім, пов'язано з тим, що принципи пошуку, які застосовуються в антивірусних програмах, не дозволяють розпізнавати нові різновиди шкідливих програм (ШП) до їх вивчення аналітиками та внесення доповнень і змін до антивірусних баз. Існуючі евристичні технології, що покликані допомогти у визначенні нових модифікацій вірусів, не дають належного рівня розпізнавання у зв'язку з їх слабкою ефективністю в процесі роботи з зашифрованими об'єктами. До недоліків існуючих методів розпізнавання ШП також можна віднести уразливість до нових атак, низьку точність і швидкість роботи. Зазначені недоліки важко усунути, використовуючи тільки традиційні способи в області комп'ютерної безпеки.

Використання методів штучного інтелекту дозволяє розпізнавати широкий клас вірусів на основі принципів навчання та адаптації баз знань до зовнішнього середовища. У цьому зв'язку у складі евристичних аналізаторів ШП зараз активно використовуються ШНМ, ШІС, МАС тощо, за допомогою яких можна ефективно розпізнавати як старі, так і нові модифікації вірусів з мінімально можливим завантаженням системи. Різним аспектам розробки, реалізації та використання методів і моделей інтелектуального розпізнавання ШП присвячені роботи Є.С. Абрамова, А.І. Аветисяна, П.П. Алексєєва, Н.О. Андреєва, Дж. Біла, Ю.А. Брюхомицького, А.В. Гаврилова, В.А. Головка, Дж. Гомеса, Ф. Гонсалеса, В.І. Городецького, С.В. Гошка, Ю.Г. Ємельянової, О.Г. Корченка, І.В. Котенка, О.В. Лукацького, Є.О. Новикова, С.А. Петрова та інших вчених.

Втім, не зважаючи на загальну методологічну основу, застосування методів і моделей ІОІ в системах комп'ютерної безпеки має свої особливості, що визначаються насамперед характером і поведінкою ШП. Одним із шляхів підвищення ефективності систем комп'ютерної безпеки є застосування гібридних підходів, що використовують властивості різних технологій ІОІ, які дозволяють створювати програмні системи, що привносять нову якість сервісу, високу ефективність і ряд інших переваг. Проте повністю ефективних способів боротьби з комп'ютерними погрозами на сьогоднішній день не існує.

У зв'язку з цим актуальною задачею як з теоретичної, так і з практичної точки зору є розробка методів і моделей розпізнавання шкідливих програм, які враховують властивості ШІС, ШНМ та МАС, що дозволяє підвищити ефективність систем комп'ютерної безпеки. Задачі, які при цьому виникають, обумовили напрям досліджень даної дисертаційної роботи.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана відповідно до плану науково-дослідних робіт Харківського національного університету радіоелектроніки (ХНУРЕ) в рамках держбюджетних тем «Еволюційні гібридні системи обчислювального інтелекту зі змінною структурою для інтелектуального аналізу даних» (№ ДР 0110U000458), розділ «Еволюційні гібридні методи та моделі інтелектуальної обробки інформації зі змінною структурою за умов невизначеності», та «Нейро-фаззі системи для поточної кластеризації і класифікації послідовностей даних за умов їх викривленості відсутніми та аномальними спостереженнями» (№ ДР 0113U000361), розділ «Адаптивні методи та моделі класифікації даних і прогнозування часових рядів за умов їх викривленості відсутніми та аномальними спостереженнями на основі штучних імунних систем», затвердженими Міністерством освіті і науки України. Автор був одним з виконавців робіт за даними темами.

Мета і задачі дослідження. Метою дисертаційної роботи є розробка, дослідження та удосконалення методів і моделей розпізнавання шкідливих програм на основі штучних імунних систем, що дозволяє створювати більш ефективні системи комп'ютерної безпеки на основі принципів навчання та адаптації баз знань до зовнішнього середовища і тим самим отримувати більш обґрунтовані рішення.

Для досягнення поставленої мети необхідно вирішити такі задачі:

– аналіз існуючих методів і моделей розпізнавання шкідливих програм;

– розробка моделі евристичного аналізатора шкідливих програм, яка використовує поведінковий аналіз на підставі даних, отриманих від емуляторів, та виконує їх інтелектуальний аналіз;

– розробка методу розпізнавання шкідливих програм на основі штучної імунної мережі та дослідження основних імунних операторів;

– розробка методу розпізнавання шкідливих програм на основі штучної нейронної мережі з імунним навчанням;

– розробка моделі штучної імунної мережі для розпізнавання шкідливих програм у вигляді мультиагентної системи;

– експериментальні дослідження розроблених методів і моделей та вирішення за їх допомогою практичних задач.

Об'єктом дослідження є процеси розпізнавання шкідливих програм.

Предметом дослідження є методи та моделі розпізнавання шкідливих програм на основі штучних імунних систем.

Методи дослідження. Для розв'язання поставлених задач були використані: теорії ШІС, ШНМ та МАС, що дозволило синтезувати нові методи та моделі розпізнавання ШП; теорії оптимізації, що дозволило розробити методи навчання та адаптації запропонованих моделей, а також апарат математичної статистики, що дозволив виконувати систематизацію та використання отриманих у роботі даних для наукових і практичних висновків.

Наукова новизна результатів дисертаційної роботи. Вирішення поставлених задач дозволило автору отримати такі результати:

1. Вперше запропоновано модель евристичного аналізатора шкідливих програм, яка виконує ймовірнісне розпізнавання на основі зваженої оцінки ознак, використовує поведінковий аналіз на підставі даних, отриманих від емуляторів, та виконує їх інтелектуальний аналіз, що дозволяє розпізнавати нові модифікації вірусів, без необхідності термінового оновлення антивірусних баз, а також звести ризик помилкових спрацьовувань до мінімуму.

2. Вперше запропоновано метод розпізнавання шкідливих програм на основі штучної імунної мережі, яка характеризується можливістю розпізнавання не одиничним антитілом або клоном, а організованою мережею взаємодіючих антитіл, що дозволяє підвищити точність і швидкість розпізнавання та виявляти не тільки потенційно шкідливий код без звернення до баз даних сигнатур, а й не відомі віруси.

3. Вперше запропоновано представлення моделі штучної імунної мережі, яка використовується для розпізнавання шкідливих програм, у вигляді мультиагентної системи, програмні агенти якої ідентифікують виконувані файли в сенсорних областях та взаємодіють між собою в комунікаційних областях, які визначаються афінностями, що узагальнює її опис, робить більш гнучкою і дозволяє змінювати параметри і структуру імунної мережі на основі розподіленої обробки з мінімально можливими витратами системних ресурсів.

4. Набув подальшого розвитку метод розпізнавання шкідливих програм на основі штучної нейронної мережі, навчання якої, на відміну від існуючих, пропонується здійснювати за допомогою штучної імунної системи з використанням моделі кодування параметрів, які настроюються, у вигляді адаптивного структурованого мультиантитіла, що призводить до підвищення ефективності її навчання за рахунок роздільного застосування імунних операторів до кожної з частин мультиантитіла та зменшення кількості нейронів у прихованих шарах.

Практичне значення результатів дисертаційної роботи. Результати дисертаційної роботи, які доведені до рівня програмних засобів, дозволяють у різних аспектах підвищити якість забезпечення комп’ютерної безпеки. Експериментальні дослідження, які проведені для оцінки працездатності та ефективності розроблених методів і моделей розпізнавання ШП, підтверджують основні положення, що виносяться на захист. Результати роботи використано для підвищення ефективності системи безпеки комп'ютерної мережі ТОВ «Іпрасофт» (акт впровадження від 21.01.2015), а також для роботи з мережевими протоколами та в системному адмініструванні ТОВ «Інтехсофт» (акт впровадження від 30.04.2015). Результати дисертаційної роботи також були використані в навчальному процесі ХНУРЕ (акт впровадження від 23.04.2015).

Особистий внесок здобувача. Всі основні результати, що виносяться на захист, отримано автором самостійно. У роботах, що опубліковані в співавторстві, здобувачеві належать: в [1] – розробка структури експертного оцінювання з використанням принципів паралелізму; в [2] – запропоновано мультиагентний підхід до вирішення задачі комівояжера; в [3] – розробка мультиагентної моделі ШІС для розпізнавання ШП; в [4] – розробка модифікованої моделі автоматичної класифікації на основі імунного методу RLAIS; в [5] – розробка нейромере-

жевого евристичного аналізатора (ЕА) ШП з імунним навчанням; в [6] – розробка моделі нечіткої класифікація об'єктів на основі ШІС; в [7] – розробка моделі автоматичної класифікації об'єктів; в [8] – синтез моделі ЕА ШП; в [9] – синтез моделі розпізнавання ШП на основі мультиагентного підходу; в [10] – запропоновано імунний підхід до класифікації об'єктів; в [11] – запропоновано середовище моделювання МАС; в [12] – запропоновано використання штучних імунних мереж (ШІМ) для розпізнавання комп'ютерних вірусів; в [13] – застосування МАС для розпізнавання комп'ютерних вірусів; в [14] – запропоновано агентно-орієнтований підхід для створення системи підтримки прийняття рішень; в [15] – використано мультиагентний підхід для вирішення задачі комівояжера; в [16] – запропоновано модель взаємодії агентів на основі ШІС; в [17] – розробка моделі взаємодії агентів в МАС з використанням ШІС; в [18] – використання ШІМ для розпізнавання ШП; в [19] – синтез моделі інтелектуальної МАС на основі ШІМ; в [20] – запропоновано МАС на основі ШІМ; в [21] – синтез МАС виявлення комп'ютерних вторгнень і розпізнавання вірусів; в [22] – підхід для розпізнавання комп'ютерних вірусів на основі ШІМ; в [23] – розробка моделі представлення МАС за допомогою ШІС; [24] – розробка структури мультиагентної моделі розпізнавання ШП; в [25] – розробка імунної моделі розпізнавання комп'ютерних вірусів на основі мультиагентного підходу; в [26] – розробка моделі ЕА ШП на основі нейронної мережі; в [27] – розробка МАС розпізнавання та запобігання вторгнень у комп'ютер; в [28] – розробка гібридної моделі ЕА ШП з використанням ШНМ; в [29] – використання адаптивного структурованого мультиантитіла для навчання нейромережевого ЕА ШП; в [30] – запропоновано навчання нейромережевого ЕА ШП за допомогою ШІС.

Апробація результатів дисертації. Основні положення та результати дисертаційної роботи доповідалися й обговорювалися на: 12–19-му Міжнародних молодіжних форумах «Радіоелектроніка та молодь у XXI столітті» (Харків, 2008-2015 рр.); 1-5-й Міжнародних науково-технічних конференціях «Сучасні напрямки розвитку інформаційно-комунікаційних технологій та засобів управління» (Харків, 2010, 2011, 2013-2015 рр.); 1-й і 2-й Міжнародних науково-технічних конференціях «Інформаційні технології в навігації і управлінні: стан та перспективи розвитку» (Київ, 2010, 2011); 9-й Міжнародній науково-практичній конференції «Математичне та програмне забезпечення інтелектуальних систем» (Дніпропетровськ, 2011); 1-й і 2-й Міжнародних науково-технічних конференціях «Проблеми інформатизації» (Київ, 2013, 2014); 2-й і 3-й Міжнародних науково-практичних конференціях «Обчислювальний інтелект» (Черкаси, 2013, 2015); Міжнародній науковій конференції «Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту – ISDMCI–2013» (Євпаторія 2013); Міжнародній науково-технічній конференції «Інформаційні проблеми теорії акустичних, радіоелектронних і телекомунікаційних систем – IPST–2013» (Алушта, 2013); 1-й і 2-й Міжнародних науково-практичних конференціях «Інформатика, математичне моделювання, економіка» (Смоленськ, 2012, 2013); Міжнародній науково-практичній конференції «Інформаційні управляючі системи та технології» (Одеса, 2014).

Публікації. За темою дисертаційної роботи опубліковано 30 наукових праць, з них: 9 статей у фахових періодичних виданнях з технічних наук (серед них 3 видання, що входять до міжнародних наукометричних баз), 1 стаття у закордонному виданні (Польща); 20 публікацій у збірниках праць і тез міжнародних науково-технічних конференцій та семінарів.

Структура та обсяг дисертаційної роботи. Дисертація складається із вступу, чотирьох розділів, висновків, списку використаних літературних джерел з 173 найменувань і 3 додатків. Робота містить 36 рисунків, 6 таблиць. Загальний обсяг роботи складає 164 сторінки, з них 138 – основного тексту.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність обраної теми дисертації, сформульовано мету та задачі дослідження, визначено об’єкт, предмет і методи досліджень, охарактеризовано наукову новизну та практичне значення отриманих результатів, а також особистий внесок автора в роботах, виконаних у співавторстві, наведено відомості про апробацію результатів дисертації та кількість публікацій за темою дисертаційної роботи.

У першому розділі проведено аналіз проблеми розпізнавання ШП, який вказав на необхідність використання нових підходів до розпізнавання, які мають базуватися на аналізі поведінки ШП і діяти в обхід шифрування на більш високому рівні. Аналіз існуючих класів вірусів показав, що сучасне шкідливе ПЗ містить широкий спектр вірусів, тому необхідно розробити методи та моделі розпізнавання як старих, так і нових модифікацій вірусів з мінімально можливим завантаженням системи, а також захищати комп’ютерні мережі без необхідності оновлення антивірусного ПЗ.

Проведений аналіз методів і моделей розпізнавання ШП показав, що сучасні системи виявлення вірусів використовують як сигнатурний, так і евристичний методи, поєднуючи в собі їх недоліки й переваги. З появою евристичних аналізаторів (ЕА) нового покоління, що використовують поведінковий аналіз на підставі даних, отримуваних від емуляторів, та їх інтелектуального аналізу, з’явилася можливість не тільки виявляти ШП без звернення до баз даних сигнатур, але й розпізнавати раніше не відомі віруси. Використання методів штучного інтелекту дозволяє створювати принципово нові моделі розпізнавання ШП, що підвищують рівень захищеності комп'ютерних систем. Розглянуто методи штучного інтелекту, які використовуються для розпізнавання ШП, аналіз яких показав, що для підвищення ефективності розпізнавання ШП доцільною є розробка методів і моделей на основі поєднання різних технологій ІОІ, в яких взаємно компенсуються їх недоліки і об’єднуються переваги. На основі проведеного аналізу сформульовано загальну задачу дослідження, визначено сукупність перспективних напрямків розпізнавання ШП на основі ШІС і сформульовано задачі дисертаційної роботи.

У другому розділі для вирішення задачі розпізнавання ШП у складі ЕА, який виконує ймовірнісне розпізнавання на основі зваженої оцінки деякої кіль-

кості ознак, пропонується використовувати ШІС, для яких виконувані файли є антигенами, а можливі вирішення задачі – антитілами. Схематично запропонована модель такого ЕА складається з блоків, наведених на рис. 1.

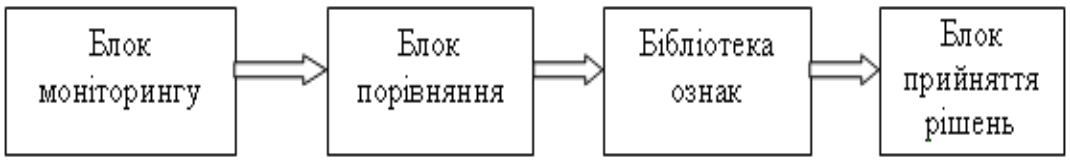

Рисунок 1 – Модель евристичного аналізатора шкідливих програм

Функцією блока моніторингу є моніторинг поведінки ШП та не ШП з метою отримання протоколу їх роботи (послідовностей виклику API функцій і переданих їм аргументів). Блок порівняння приймає протоколи роботи декількох програм від блока моніторингу і порівнює їх. Результатом роботи є множина однакових фрагментів (ознак) у протоколах різних програм одного сімейства. Бібліотека ознак зберігає в собі всі ознаки, виявлені блоком порівняння, і веде статистику їх появи, на основі якої кожній ознаці присвоюється рейтинг. Функція блока прийняття рішень – прийняття рішення про належність чи неналежність розглянутої програми до деякого сімейству ШП. Він може бути реалізований з використанням різних технологій ІОІ, зокрема, на основі ШІС, ШНМ, МАС тощо.

Для розпізнавання ШП необхідно обрати перелік ознак, за якими це розпізнавання проводитиметься. Щоб ефективно розпізнати шкідливий код, необхідно скласти бібліотеку подій, якими є програмні дії, пов'язані з системними викликами, що призводять до змін у системі. Події, що найбільш часто зустрічаються у ШП, і не зустрічаються в не ШП, і будуть характерними ознаками.

Для реалізації ЕА на основі ШІС був проведений аналіз її основних математичних моделей (модель негативного/позитивного відбору, модель клонального відбору та модель ШІМ), який показав, що для розпізнавання ШП найбільш придатною є модель ШІМ, яка дозволяє розпізнавати ШП не поодиноким антитілом або клоном, а організованою мережею взаємодіючих антитіл, що дозволяє підвищити швидкість і точність розпізнавання та виявляти не тільки потенційно шкідливий код без звернення до баз даних сигнатур, а й не відомі віруси. Модель ШІМ за розпізнаванням ШП подано у такий спосіб:

$$\begin{aligned} \text{AINet} = (Ag, Ab, T, s) = [&Present(Ag, Ab) \rightarrow Select(Ab) \rightarrow \\ &\rightarrow Clon(Ab) \rightarrow Mut(Cl) \rightarrow Present(Ag, Cl) \rightarrow \\ &\rightarrow MemForm(Cl) \rightarrow Suppr(Ab, Cl, s)] \rightarrow TermTest(T), \end{aligned} \quad (1)$$

де Ag – популяція антигенів; Ab – популяція антитіл; T – критерій зупинки; s – поріг близькості. В циклі виконується така послідовність імунних операторів: $Present(Ag, Ab)$ – оператор представлення антитіл Ab антигенам Ag шляхом обчислення афінностей між ними:

$$Aff_{Ab_i - Ag} = (1 + d_{Ab_i - Ag})^{-1}, \quad (2)$$

де d_{ab_i-ab} – відстань між i-м антитілом $Ab_i, i=\overline{1,M}$ та всіма антигенами Ag:

$$d_{Ab_i-Ag} = \|Ab_i - Ag\| = \sqrt{\sum_{j=1}^{F}(Ab_i - Ag_j)^2}, i=\overline{1,M}. \quad (3)$$

$Select(Ab)$ – оператор відбору антитіл з найкращою афінністю; $Clon(Ab)$ – оператор клонування відібраних антитіл та формування популяції клонів Cl; $Present(Ag,Cl)$ – оператор представлення популяції клонів Cl антигенам Ag шляхом обчислення афінностей згідно з (2); $MemForm(Cl)$ – формування пам'яті клонів з найкращою афінністю; $Suppr(Ab,Cl,s)$ – оператор супресії ШІМ шляхом обчислення афінностей, схожих з (2), між всіма антитілами і клонами, та видалення тих антитіл і клонів, для яких афінність перевищує поріг близькості s; $TermTest(T)$ – процедура перевірки критерію закінчення роботи алгоритму T.

Досліджено вплив основних імунних операторів (клонування та мутації антитіл) на швидкість збіжності імунних алгоритмів, що використовуються для розпізнавання ШП. Удосконалено підходи до виконання клонування та мутації антитіл для випадку дійсного кодування. Показано вплив параметрів оператора клонування (кількість антитіл для клонування і кратність клонування) на збіжність імунних алгоритмів. Із збільшенням значень даних параметрів зменшується кількість поколінь, необхідних для збіжності імунного алгоритму. Проте слід зазначити, що час обчислень для кожного покоління збільшується пропорційно збільшенню кількості клонів. Тому необхідно регулювати параметри оператора клонування в процесі роботи алгоритму.

Кількість антитіл для клонування в імунних алгоритмах, що використовуються для розпізнавання ШП, є фіксованою. Кратність клонування антитіла регулюється в процесі роботи імунного алгоритму пропорційно афінності:

$$N_c(Ab_i) = \begin{cases} N_{c\_\min}, \ якщо \ Aff(Ab_i) \le Aff_{best} * 0.3, \\ N_{c\_\max}, \ якщо \ Aff(Ab_i) \ge Aff_{best} * 0.7, \\ \alpha * N_{c\_\min} + (1-\alpha) * N_{c\_\max}, \ в \ інших \ випадках, \end{cases} \quad (4)$$

де $\alpha = \dfrac{Aff(Ab_i) - Aff_{best} * 0.3}{Aff_{best} * 0.4}$; $N_{c\_\min}$ та $N_{c\_\max}$ – мінімальна та максимальна кратності клонування антитіла відповідно; $Aff(Ab_i)$ – значення афінності антитіла Ab_i; Aff_{best} – краще значення афінності в поточному поколінні.

Використання дійсного кодування антитіл у запропонованих імунних алгоритмах розпізнавання ШП вимагає визначення оператора мутації, що оперує такими параметрами, як імовірність і крок мутації. Ймовірність мутації обчислюється відповідно до афінності антитіла за виразом:

$$p_{mut}(Ab_i) = \beta * P_{mut\_max} + (1-\beta) * P_{mut\_min}, \quad (5)$$

де $\beta = \dfrac{Aff_{best} - Aff(Ab_i)}{Aff_{best} - Aff_{worst}}$; $Aff(Ab_i)$ – значення афінності антитіла Ab_i; Aff_{best} і Aff_{worst} – відповідно краще та гірше значення афінності в поточному поколінні; P_{mut_min} і P_{mut_max} – мінімальна та максимальна ймовірність мутації антитіла.

Настроювання кроку мутації виконується згідно з виразом:

$$\sigma_{i+1} = \sigma_i \frac{Aff_{best} - Aff(Ab_i)}{Aff_{best} - Aff_{worst}}. \qquad (6)$$

Таким чином, величина кроку мутації та ймовірність мутації антитіл регулюються залежно від афінностей у процесі роботи імунного алгоритму.

Запропонований ЕА працює в двох режимах: навчання та розпізнавання. У режимі навчання відбувається настроювання ЕА на розпізнавання поведінки ШП, при цьому виконуються наступні дії. Множина файлів, що виконуються і належать до одного сімейства, досліджується за допомогою емуляції і складаються докладні карти їхніх дій (протоколи). Протоколи порівнюються між собою для виявлення загальних закономірностей у поведінці об’єктів. Знайдені закономірності подаються у вигляді фрагментів протоколів і зберігаються в бібліотеці. Підраховується рейтинг появи для кожного знайденого фрагмента, що показує, в якій кількості об’єктів, з усієї множини представлених був знайдений даний фрагмент. Відбувається формування вибірки з рейтингами ознак ШП для навчання ШІМ на позитивні вердикти.

Вибірка не ШП досліджується за допомогою емуляції аналогічно. Після цього в протоколах роботи не ШП проводиться пошук фрагментів поведінки ШП, попередньо збережених у бібліотеці. Для всіх не ШП так само формується вибірка з рейтингами ознак ШП, яка використовується для навчання ШІМ на негативні вердикти. Створюється та навчається ШІМ на раніше підготовлених наборах рейтингів появи ознак. При цьому виконується кластеризація вхідної множини даних на дві підмножини, перша з яких відповідатиме ШП досліджуваного сімейства, а друга – не ШП або ж ШП іншого сімейства. ШІМ, що навчена, представляється множиною антитіл пам’яті $Ab_{\{m\}}$ і матрицею їх афінностей B. Множина інтерпретує внутрішні відображення антигенів, які подані на вхід мережі. Матриця афінностей описує зв’язки між антитілами і показує загальну структуру ШІМ.

Шляхом вимірювання афінностей антитіл з множини клітин пам’яті до антигенів з навчального набору можна визначити, які з антитіл розпізнають антигени, відповідні ШП з даного сімейства, а які – розпізнають не ШП (або ШП інших сімейств).

У режимі розпізнавання виконуваний файл досліджується за допомогою емулятора. У протоколі досліджуваного файлу здійснюється пошук фрагментів поведінки ШП з бібліотеки ознак, з якої беруться рейтинги для віднайдених фрагментів. Рейтинги подаються на входи ШІМ, яка виносить вердикт про належність досліджуваного об’єкта до класу ШП чи до класу не ШП.

У третьому розділі розглянуто питання розпізнавання ШП на основі нейромережевого та мультиагентного підходів. Оскільки необхідно розпізнавати ШП різних сімейств, то ЕА складається з декількох паралельно працюючих нейронних мереж (НМ), кожна з яких орієнтована на певне сімейство ШП. На входи НМ подаються рейтинги ознак, а вихідний сигнал відповідної НМ призначений для розпізнавання ШП певного сімейства.

Аналіз існуючих видів НС показав, що для вирішення задачі розпізнавання ШП достатньо використовувати багатошаровий (тришаровий) персептрон, нейрони проміжного шару якого мають сигмоїдальну функцію активації:

$$z_m = f(u_m) = \frac{1}{1+e^{-\lambda_m u_m}}, \qquad u_m = \sum_{n=1}^{N} w_{n,m} x_n + w_{o,m}, \tag{7}$$

де $z_m, m = \overline{1,M}$ – вихідний сигнал m-го нейрона проміжного шару, який складається з M нейронів, що мають N виходів; $x_n, n = \overline{1,N}$ – n-а компонента вхідного вектора ознак, що подається на вхідний шар НМ; $w_{n,m}$ – ваговий коефіцієнт n-ї вхідної ознаки, що надходить на вхід m-го нейрона проміжного шару; $w_{o,m}$ – значення зміщення; λ_m – коефіцієнт, що визначає крутизну функції активації $f(u_m)$. Нейрон вихідного шару має порогову функцію активації:

$$y_k = \varphi\left(\sum_{m=1}^{M} v_m \cdot z_m + v_o\right) = \begin{cases} 1, & якщо \ \ y_k > 0, \\ 0, & якщо \ \ y_k \le 0, \end{cases} \tag{8}$$

де v_m – вагові коефіцієнти; v_o – зміщення.

Для навчання НМ можуть бути використані різні методи. Існуючі методи навчання є трудомісткими, а також висувають значні математичні вимоги до видів цільових функцій та обмежень. Основною їх рисою є відсутність можливості зміни кількості нейронів у проміжному шарі. Для усунення недоліків існуючих методів навчання НМ пропонується використання ШІС.

Задача навчання всіх параметрів НМ вирішується в режимі off-line. Формується популяція антигенів $Ag = \{Ag_1, Ag_2, ..., Ag_S\}$, де S – розмір популяції, що відповідає кількості прикладів у навчальній вибірці. Кожен елемент множини Ag – приклад з навчальної вибірки, представлений у вигляді вектора фіксованої довжини $Ag_i = \langle x_1^i, x_2^i, ..., x_n^i, y^i \rangle, i = \overline{1,S}$, де $x_1^i, x_2^i, ..., x_n^i$ – вхідні змінні; y^i – вихідна змінна для i-го прикладу навчальної вибірки. Як антитіла використовуються вектори параметрів, що настроюються. В одному антитілі кодуються всі параметри НС: $w_{n,m}$, $w_{o,m}$, v_m, v_o та λ_m, $n = \overline{1,N}$ $m = \overline{1,M}$. Використовується дійсне кодування антитіл, при якому кожен параметр вектора антитіла описується окремим дійсним числом. Для вирішення задачі навчання пропонується використання моделі кодування параметрів, що настроюються, у вигляді адаптивного структурованого мультиантитіла, що складається з двох частин, кожна з яких може оброблятися незалежно одна від одної (рис. 2).

$w_{1,1},\ldots,w_{1,M};\ldots,w_{N,1},\ldots,w_{N,M};w_{0,1},\ldots,_{0,M};\lambda_1,\ldots,\lambda_M$	v_1	…	v_M	v_0
ab_0	ab_1	…	ab_M	ab_{M+1}
Частина 1	Частина 2			

Рисунок 2 – Структура мультиантитіла mAb

Популяція мультиантитіл подана у вигляді $mAb=\{mAb_1,mAb_2,\ldots,mAb_N\}$, де $mAb_i=\{ab_0,ab_1,ab_2,\ldots,ab_{L-1}\}$ $i=\overline{1,N}$ – i-е адаптивне мультиантитіло, що являє собою структурований вектор, довжина якого змінюється в процесі виконання імунного алгоритму.

Кожне мультиантитіло mAb_i, $i=\overline{1,N}$ популяції характеризується повною множиною параметрів НМ, що настроюються. У частині 1 мультиантитіла закодовані вагові коефіцієнти $w_{n,m}$, значення зсувів $w_{o,m}$ і коефіцієнти λ_m. У частині 2 закодовані коефіцієнти v_m і зміщення v_o. Друга частина мультиантитіла є адаптивною, тому в процесі навчання крім оптимізації коефіцієнтів, що містяться в цій частині, змінюється і їх загальна кількість, що, в свою чергу, призводить до зміни кількості нейронів у прихованому шарі нейронної мережі. Структурований спосіб формування мультиантитіла дозволяє підвищити ефективність імунного алгоритму за рахунок роздільного застосування імунних операторів до кожної з частин антитіла.

Обчислення афінності виконується для мультиантитіла в цілому:

$$Aff_{mAb-Ag}=(1+d_{mAb-Ag})^{-1}, \tag{9}$$

де d_{mAb-Ag} – відстань Хеммінга між отриманим значенням виходу НМ $y_s, s=\overline{1,S}$ і бажаним y для всіх s антигенів популяції Ag:

$$d_{mAb-Ag}=\sum_{s=1}^{S} y_s,\ де\ \ y_s=\begin{cases}1,\ якщо\ y_s\neq y,\\ 0,\ якщо\ y_s=y.\end{cases} \tag{10}$$

Обчислення афінності антитіл всередині частини 2 мультиантитіла виконується за виразом:

$$Aff_{ab_i-ab}=(1+d_{ab_i-ab})^{-1}, \tag{11}$$

де d_{ab_i-ab} – відстань між i-м антитілом та іншими антитілами частини 2 мультиантитіла:

$$d_{ab_i-ab}=\left\|ab_i-ab_j\right\|=\sqrt{\sum_{j=1}^{M}(v_i-v_j)^2}, i=\overline{1,M}\,. \tag{12}$$

Виконання супресії шляхом видалення антитіл ab_i з афінністю, більшою заданого порогу δ_{net}, дозволяє зменшити кількість нейронів у прихованому шарі та усунути, таким чином, надмірність мережі.

У роботі розпізнавання ШП пропонується здійснювати за допомогою МАС. Загальна модель МАС розпізнавання ШП (MASRM – Multi-Agent System for Recognition of Malwares) може бути формально представлена кортежем:

$$MASRM = \langle El, Attr, Env, Rl, RAct, CAct, Ev \rangle, \quad (13)$$

де $El = \langle Ob \cup AgD \cup AgA \rangle$ – множина елементів системи, що складається з об'єктів (виконуваних файлів) $Ob = [P_1, P_2, ... P_F]$, агентів-детекторів $AgD = [H_1, H_1, ..., H_N]$, $H_n \in Q$, $n = \overline{1,N}$ для виявлення ШП, та агентів-аналізаторів $AgA = [G_1, G_1, ..., G_M]$, $G_m \in Q$, $m = \overline{1,M}$ для розпізнавання ШП.

МАС розпізнавання ШП може бути представлена структурою (рис. 3):

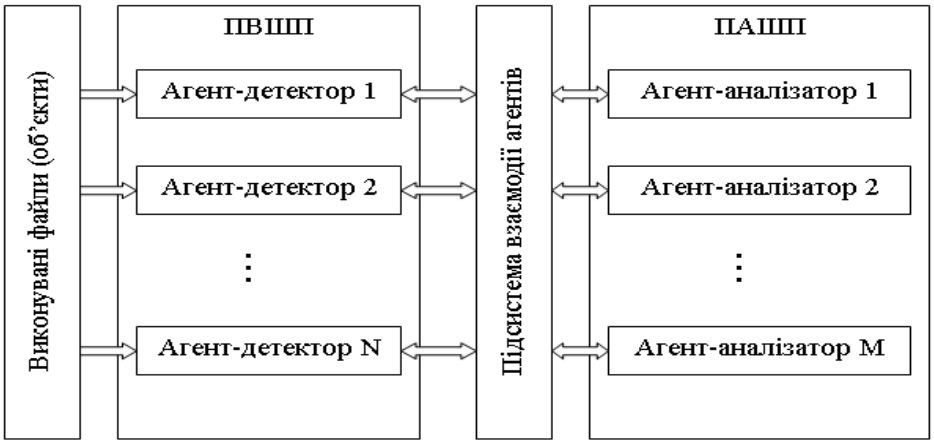

Рисунок 3 – Структура МАС розпізнавання шкідливих програм

У запропонованій структурі МАС можна виділити дві основні підсистеми: 1) підсистему виявлення ШП (ПВШП); 2) підсистему аналізу ШП (ПАШП). Обидві підсистеми складаються з набору агентів, кожен з яких працює незалежно один від одного і вирішує загальну задачу, покладену на систему. Виділена окрема підсистема, що відповідає за взаємодію агентів.

У пропонованій МАС розпізнавання ШП використовуються два види агентів: агент-детектор і агент-аналізатор. Основне завдання агента-детектора – моніторинг основних вразливостей ОС, і в разі виявлення аномальної активності – розміщення інформації про процес на «дошці оголошень». Агент-аналізатор є інтелектуальним програмним агентом, який використовує евристичний аналіз. Завдання агента-аналізатора – дослідження процесів, розміщених на «дошці оголошень», і прийняття рішення, які з процесів є потенційними вірусами і до якого класу ШП вони належать.

У роботі запропонована модель подання ШІМ, що використовується для розпізнавання ШП, у вигляді МАС (MAMAIN – Multi-Agent Model of Artificial Immune Network), яка подана на рис. 4 та описується наступним кортежем:

$$MAMAIN = \langle El, Attr, Env, Rl, SNs, CNs, RAct, CAct, Ev \rangle, \quad (14)$$

де El – множина елементів системи, що характеризуються набором атрибутів-

ознак (фрагментів програм) $Attr$ і функціонують у навколишньому середовищі Env, яка являє собою ОС комп'ютера, знаходяться в певних відносинах Rl, що дозволяють взаємодіяти один з одним в сенсорних SNs та комунікаційних CNs областях, мають можливість виконувати реактивні $RAct$ і комунікативні $CAct$ дії для досягнення мети, змінюючи свої атрибути $Attr$ в процесі еволюції Ev.

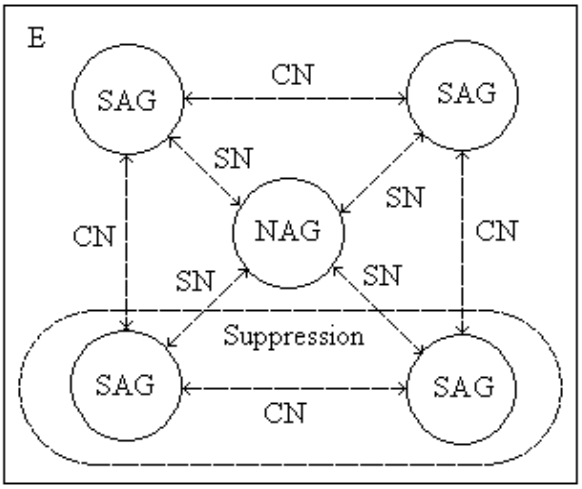

Рисунок 4 – Модель подання ШІМ у вигляді МАС

У моделі подання ШІМ у вигляді МАС використовуються тільки два типи агентів: антигени N_j, $j=\overline{1,M}$, подані як non-self агенти ($NAGs$), а антитілам S_i, $i=\overline{1,N}$ відповідають self агенти ($SAGs$). Отже, множина елементів El МАС складається з self агентів $SAGs$ та non-self агентів $NAGs$ ($El = SAG_i \cup NAG_j$), кожен з яких характеризується набором атрибутів-ознак $\{a_{jk}\}$ і $\{b_{il}\}$, $i=\overline{1,N}$, $j=\overline{1,M}$, $k=\overline{1,m}$, $l=\overline{1,n}$.

Модель розпізнавання ШП на основі МАС, яка описує ШІМ (MAMAIN), може бути представлена такою послідовністю виконання операторів:

$$\begin{aligned} &MAMAIN(NAGs, SAGs, Aff_{SN}, Aff_{SS}, SNs, CNs, T_{NAG}, T_{SAG}, p) = \\ &= NAGpres(NAGs, SAGs, Aff_{SN}) \to SAGsel(SAGs, SNs, T_{NAG}) \to \\ &\to SAGs_{Cl}[Clon(SAGs, T_{NAG}) \to Mut(SAGs_{Cl}) \to \\ &\to Clpres(NAGs, SAGs_{Cl}, Aff_{SN}) \to Clsel(SAGs_{Cl}, SNs, T_{NAG}) \to \\ &\to SAGpres(SAGs, SAGs_{Cl}, Aff_{SS}) \to Supp(SAGs, SAGs_{Cl}, CNs, T_{SAG}) \to \\ &\to Age(SAGs, SAGs_{Cl}) \to TermTest(p)], \end{aligned} \tag{15}$$

де $NAGpres(NAGs, SAGs, Aff_{SN})$ – оператор представлення self агентів $SAGs$ non-self агентам $NAGs$; $SAGsel(SAGs, SNs, T_{NAG})$ – оператор відбору self агентів $SAGs$; $Clon(SAGs, T_{NAG})$ – оператор клонування відібраних self агентів $SAGs$; $Mut(SAGs_{Cl})$ – оператор мутації клонів; $Clpres(NAGs, SAGs_{Cl}, Aff_{SN})$ – оператор

представлення клонованих self агентів $SAGs_{cl}$ non-self агентам $NAGs$; $Clsel(SAGs_{Cl}, SNs, T_{NAG})$ – оператор відбору клонованих self агентів $SAGs_{cl}$; $SAGpres(SAGs, SAGs_{Cl}, Aff_{SS})$ – оператор представлення відібраних $SAGs$ і клонованих $SAGs_{cl}$ self агентів один одному; $Supp(SAGs, SAGs_{Cl}, CNs, T_{SAG})$ – оператор супресії self агентів; $Age(SAGs, SAGs_{Cl})$ – оператор старіння; $TermTest(p)$ – процедура перевірки критерію зупинки.

Запропоноване подання ШІМ, що використовується для розпізнавання ШП, у вигляді МАС, узагальнює її опис, робить більш гнучкою і дозволяє змінювати її параметри і структуру на основі розподіленої обробки.

У четвертому розділі розглянуті питання створення інструментальних засобів для моделювання роботи ЕА та проведення експериментальних досліджень. Запропоновано інструментальне середовище моделювання, яке забезпечує можливість впровадження розроблених методів і моделей у різних практичних задачах та підвищення ефективності систем комп'ютерної безпеки.

Для моделювання роботи ЕА обраний спеціалізований набір інструментів. Моделювання блока моніторингу ЕА виконувалося з використанням емулятора системи Microsoft Windows – iMUL. Дане ПЗ емулює роботу центрального процесора, API функцій ОС та її внутрішніх структур. Моделювання блока порівняння ознак проводилося за допомогою спеціально розроблених для цього утиліт Threader і Matcher. Дані утиліти призначені для перетворення і дослідження інформації. Threader є консольним додатком, вхідні дані для його роботи – протокол емулятора в текстовому вигляді. Matcher також є консольним додатком, вихідні дані для його роботи – файли, створені програмою Threader.

Моделювання роботи ШНМ виконано за допомогою аналітичної платформи Deductor. Реалізовані в Deductor технології дозволяють на базі єдиної архітектури пройти всі етапи побудови аналітичної системи – від створення сховища даних до автоматичного підбору моделей і візуалізації отриманих результатів. Моделювання ШІМ aiNet проводилося за допомогою програмного пакета Scilab 5.5. Аналіз даних, отриманих внаслідок навчання ШІМ aiNet, а також розпізнавання нових антигенів проводилося за допомогою спеціально розробленої утиліти aiNet_Help_Tool.

Як тестові були розглянуті задачі розпізнавання ШП різних сімейств з використанням ШІМ, ШНМ та МАС. При цьому ШІМ і ШНМ дають однакову точність детектування нових модифікацій ШП, процес навчання ШІМ відбувається швидше, ніж ШНМ, а за швидкістю детектування нових модифікацій ШП вже навчена ШНМ перевершує ШІМ. Крім того, МАС визначає ШП з меншим споживанням системних ресурсів порівняно з нейромережевим та імунним підходами. Проведено порівняльний аналіз розроблених методів і моделей розпізнавання ШП з існуючими антивірусними програмами (NOD32, Avast та Касперського) на різних сімействах вірусів, який показав, що запропоновані підходи на деяких сімействах ШП дають кращі результати, ніж існуючі.

У **додатку** наведено акти про використання результатів дисертаційної роботи для вирішення практичних задач та у навчальному процесі.

ВИСНОВКИ

У дисертаційній роботі наведено результати, які, згідно з метою дослідження, в сукупності є вирішенням актуальної наукової задачі – розробки методів і моделей розпізнавання шкідливих програм на основі штучних імунних систем, що має велике значення для підвищення ефективності систем комп'ютерної безпеки. Внаслідок проведених досліджень і вирішення поставлених задач отримано такі результати:

1. Нова узагальнена модель ЕА, що виконує ймовірнісне розпізнавання ШП на основі зваженої оцінки деякої кількості ознак, яка використовує поведінковий аналіз на підставі даних, отримуваних від емуляторів, і виконує аналіз за допомогою різних інтелектуальних технологій, використання якої дозволяє визначати нові модифікації вірусів, а також звести ризик помилкових спрацьовувань до мінімуму.

2. Запропоновано розпізнавання ШП на основі ШІМ, яка дозволяє розпізнавати ШП організованою мережею взаємодіючих антитіл, що дає можливість підвищити точність і швидкість розпізнавання та виявляти не тільки потенційно шкідливий код без звернення до баз даних сигнатур, а й не відомі віруси.

3. Запропоновано реалізацію ЕА ШП на основі ШНМ, навчання якої здійснюється за допомогою ШІС з використанням моделі кодування параметрів, які настроюються, у вигляді адаптивного структурованого мультиантитіла, що призводить до підвищення ефективності її навчання за рахунок роздільного застосування імунних операторів до кожної з частин мультиантитіла та зменшення кількості нейронів у прихованих шарах.

4. Нова модель розпізнавання ШП у вигляді МАС на основі організації взаємодій як між програмними агентами і файлами, що виконуються, так і програмних агентів між собою, яка дозволяє розпізнавати віруси з мінімально можливими витратами системних ресурсів.

5. Нове подання моделі ШІМ у вигляді МАС, програмні агенти якої ідентифікують виконувані файли в сенсорних областях та взаємодіють між собою в комунікаційних областях, які визначаються афінностями, що робить її легко масштабованою і більш узагальненою та дозволяє змінювати параметри і структуру ШІМ на основі розподіленої обробки.

6. Проведено порівняльний аналіз розроблених методів і моделей розпізнавання ШП як між собою, так і з існуючими для різних сімейств вірусів, який показав, що МАС визначає ШП з меншим споживанням системних ресурсів порівняно з нейромережевим та імунним підходами, а запропоновані підходи на деяких сімействах ШП дають кращі результати, ніж існуючі.

7. Нейромережевий ЕА ШП з імунним навчанням використано для підвищення ефективності системи безпеки комп'ютерної мережі ТОВ «Іпра-софт», а ЕА шкідливого коду на основі ШІМ використано для роботи з мережевими протоколами і в системному адмініструванні ТОВ «Інтехсофт».

Результати роботи також використано у навчальному процесі Харківського національного університету радіоелектроніки.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Аксак Н.Г. Система параллельно-распределенного экспертного оценивания / Н.Г. Аксак, А.Ю. Лебёдкина, М.В. Кушнарёв // Вісник ХНТУ. – Херсон: ХНТУ, 2011. – №2 (41). – С. 403-407.

2. Кораблев Н.М. Агентно-ориентированный подход на основе искусственных иммунных систем для решения задачи коммивояжера / Н.М. Кораблёв, Г.С. Иващенко, М.В. Кушнарев // Бионика интеллекта: науч.-техн. журнал. – 2012. – № 2 (79). – С. 33-37.

3. Кораблев Н.М. Мультиагентная модель искусственной иммунной системы для распознавания вредоносных программ / Н.М. Кораблев, М.В. Кушнарев // Бионика интеллекта: науч.-техн. журнал. – 2014. – № 1 (82). – С. 90-94.

4. Кораблев Н.М. Модификация иммунного метода RLAIS для автоматической классификации объектов / Н.М. Кораблев, А.А. Фомичев, М.В. Кушнарев // Проблеми інформаційних технологій: наук.-техн. журнал. – 2014. – № 2 (16). – С. 29-38. (Входить до міжнародних наукометричних баз AcademicKeys, OAIJ, Research Bible).

5. Кораблев Н.М. Нейросетевой эвристический анализатор вредоносных программ с иммунным обучением / Н.М. Кораблев, М.В. Кушнарев, Д.П. Ужвий // Радиоэлектроника и информатика: научно-техн. журнал. – 2014. – № 2 (65). – С. 19-25.

6. Кораблёв Н.М. Нечеткая классификация объектов на основе искусственных иммунных систем / Н.М. Кораблев, А.А. Фомичев, М.В. Кушнарев // Наук. вісник Чернівецького ун-ту «Комп'ютерні системи та компоненти»: збірник наукових праць. – 2010. – Вип.2. – Том 1. – С. 88-94.

7. Бритик В.И. Проекционный метод автоматической классификации с использованием таксономических алгоритмов / В.И. Бритик, Н.М. Кораблев, М.В. Кушнарев // Системи управління, навігації та зв'язку. –2012.– Вип. 1 (21).– Том 2. – С. 74-80.

8. Кораблев Н.М. Модель эвристического анализатора вредоносных программ на основе искусственной иммунной сети / Н.М. Кораблев, М.В. Кушнарев // Системи обробки інформації. – 2013. – Вип. 8 (115). – С. 216-222. (Входить до міжнародної наукометричної бази Index Copernicus).

9. Кораблёв Н.М. Обнаружение и анализ вредоносных программ с использованием мультиагентного подхода / Н.М. Кораблёв, М.В. Кушнарев, О.Г. Лебедєв // Збірник наукових праць Харківського університету Повітряних Сил. – 2015. – Вип. № 1 (42). – С. 42-47. (Входить до міжнародної наукометричної бази Google Scholar).

10. Korablyov M. The immune method for classifying objects on the basis of the target clonal selection (Immunologiczne metody klasyfikacji obiektów bazujące na selekcji klonalnej) / M. Korablyov, O. Fomichov, M. Kushnaryov, W. Wójcik // Elektronika (LIV). – 2013. – № 8. – P. 34-38.

11. Коргут С.А. Среда моделирования многоагентных систем

/ С.А. Коргут, М.В. Кушнарев, К.А. Лавриненко // Сучасні напрями розвитку інформаційно–комунікаційних технологій та засобів управління. Матеріали першої наук.-техн. конференції. – Х.: ДП «ХНДІ ТМ»; К.: ДП «ЦНДІ НіУ», 2010. – С. 80.

12. Корнев А.С. Обнаружение компьютерных вирусов на основе использования искусственных иммунных сетей / А.С. Корнев, М.В. Кушнарев // 14-й міжнародний молодіжний форум «Радіоелектроніка і молодь в XXI ст.»: Зб. Матеріалів форуму. Ч.2. – Харків: ХНУРЕ, 2010. – С. 43.

13. Кораблев Н.М. Применение многоагентной системы для классификации компьютерных вирусов / Н.М. Кораблев, М.В. Кушнарев // Тези доповідей 2-ї міжнар. наук.-технічної конференції «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. – К.: ДП «ЦНДІ НіУ»; Х.: ДП «ХНДІ ТМ»; К.: КДАВТ, 2011. – С. 37.

14. Лавриненко К.А. Агентно-ориентированный подход к созданию системы поддержки принятия решений / К.А. Лавриненко, М.В. Кушнарев // Інформаційні технології в навігації і управлінні: стан і перспективи розвитку. Матеріали другої міжнар. наук.-технічної конференції. – К.: ДП «ЦНДІ НіУ», 2011. – С. 40.

15. Кораблев Н.М. Использование агентно-ориентированного подхода при решении задачи коммивояжера / Н.М. Кораблев, Г.С. Иващенко М.В. Кушнарев // IX міжнародна науково-практична конференія «Математичне та програмне забезпечення інтелектуальних систем»: тези доповідей. – Дніпропетровськ, 2011. – С. 137-138.

16. Кубиря А.В. Модели взаимодействия агентов на основе искусственных иммунных систем / А.В. Кубиря, М.В. Кушнарёв // 16-й Международный молодежный форум «Радиоэлектроника и молодежь в XXI веке». Сб. Материалов форума. Т.10. – Харьков: ХНУРЭ, 2012. – С. 23-24.

17. Кораблев Н.М. Взаимодействие агентов в мультиагентной системе с использованием искусственных иммунных систем / Н.М. Кораблев, М.В. Кушнарев, И.О. Кальницкий, Р.И. Подоляка // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: Матеріали третьої міжнар. наук.-техн. конференції, 11-12 квітня 2013 р. – Харків: ДП «ХНДІ ТМ», 2013. – С. 51.

18. Кораблев Н.М. Использование искусственной иммунной сети для обнаружения и анализа вредоносных программ / Н.М. Кораблев, М.В. Кушнарев, М.В. Мартынов // Перша міжнародна науково-технічна конференція «Проблеми інформатизації». Тези доповідей. – Черкаси–Київ–Тольятті–Харків, 2013. – С. 51-52.

19. Кораблев Н.М. Модель интеллектуальной мультиагентной системы на основе искусственной иммунной сети / Н.М. Кораблев, М.В. Кушнарев // Интеллектуальные системы принятия решений и проблемы вычислительного интеллекта: Материалы междунар. научной конференции. – Херсон: 2013. – С. 456-457.

20. Кораблев Н.М. Мультиагентная система на основе искусственной им-

мунной сети / Н.М. Кораблев, М.В. Кушнарев // Тези доповідей другої Міжнар. науково-техн. конф. «Інформаційні проблеми теорії акустичних, радіоелектронних і телекомунікаційних систем IPST-2013» 29 вересня-2 жовтня 2013 р., Алушта. – Харків, НТУ «ХПІ», 2013. – С. 50-51.

21. Кораблев Н.М. Мультиагентная система обнаружения компьютерных вторжений и распознавания вирусов / Н.М. Кораблев, Т.А. Киктенко, М.В. Кушнарев // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: Матеріали третьої міжнар. наук.-техн.конференції, 11-12 квітня 2013 р. – Харків: ДП «ХНДІ ТМ», 2013. – С. 50.

22. Кораблев Н.М. Обнаружение и анализ компьютерных вирусов на основе искусственной иммунной сети / Н.М. Кораблев, М.В. Кушнарев, Т.А. Киктенко // Сборник научных статей по итогам 2-й Междунар. научно-практ. конф. «Информатика, математическое моделирование, экономика».– Том 2. – Смоленск, 2013. – С. 30-35.

23. Кораблев Н.М. Представление мультиагентной системы с помощью искусственной иммунной системы / Н.М. Кораблев, М.В. Кушнарев // Матеріали 2-ї Міжнародної науково-технічної конференції «Обчислювальний інтелект (ОІ-2013)», (14-17 травня 2013 м. Черкаси). – Черкаси: Маклаут, 2013. – С. 107.

24. Киктенко Т.А. Использование мультиагентного подхода в задачах обнаружения вредоносного кода / Т.А. Киктенко, М.В. Кушнарев, М.В. Мартынов // 17-й Международный молодежный форум «Радиоэлектроника и молодежь в XXI веке». Сб. Материалов форума. Т.5. – Харьков: ХНУРЭ, 2014. – С.202-203.

25. Кораблев Н.М. Иммунная модель обнаружения компьютерных вирусов на основе мультиагентного подхода / Н.М. Кораблев, М.В. Кушнарев, М.В. Мартынов // Друга міжнародна науково-технічна конференція «Проблеми інформатизації». Тези доповідей. – Київ–Полтава–Катовице–Париж–Білгород–Черкаси–Харків, 2014. – С. 73.

26. Кораблев Н.М. Эвристический анализатор вредоносных программ на основе нейронной сети / Н.М. Кораблев, М.В. Кушнарев, Д.П. Ужвий // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: Матеріали четвертої міжнар. наук.-техн.конференції, 4-5 грудня 2014 р. – Полтава: ПНТУ; Баку: ВА ЗС АР; Бєлгород: НДУ «БєлДУ»; Кіровоград: КЛА НАУ; Харків: ДП «ХНДІ ТМ», 2014. – С. 36-37.

27. Кушнарев М.В. Мультиагентная система обнаружения и предотвращения вторжений в компьютер / М.В. Кушнарев, М.В. Мартынов // 18-й Международный молодежный форум «Радиоэлектроника и молодежь в XXI веке». Сб. Материалов форума. Т.3. – Харьков: ХНУРЭ, 2014. – С. 176-177.

28. Кораблев Н.М. Гибридная модель эвристического анализатора вредоносных программ / Н.М. Кораблев, М.В. Кушнарев, Д.П. Ужвий // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: Матеріали п’ятої міжнар. наук.-техн.конференції, 23-24 квітня 2015 р. – Полтава: ПНТУ; Баку: ВА ЗС АР; Бєлгород: НДУ «БєлДУ»; Кіровоград: КЛА НАУ; Харків: ДП «ХНДІ ТМ», 2015. – С. 27.

29. Кораблев Н.М. Использование адаптивного структурированного мультиантитела для обучения нейросетевого анализатора вредоносных программ / Н.М. Кораблев, М.В. Кушнарев // Обчислювальний інтелект (результати, проблеми, перспективи): Матеріали ІІІ-ї Міжнародної науково-практичної конференції. – Черкаси, 2015. – С. 84-85.

30. Кушнарев М.В. Обучение нейросетевого эвристического анализатора вредоносных программ с помощью искусственных иммунных систем / М.В. Кушнарев, Д.П. Ужвий // 19-й Международный молодежный форум «Радиоэлектроника и молодежь в XXI веке». Сб. Материалов форума. Т.5. – Харьков: ХНУРЭ, 2015. – С. 154-155.

АНОТАЦІЯ

Кушнарьов М.В. Методи та моделі розпізнавання шкідливих програм на основі штучних імунних систем. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.23 – системи та засоби штучного інтелекту. – Харківський національний університет радіоелектроніки, Міністерство освіти і науки України, Харків, 2016.

Запропоновано узагальнену модель евристичного аналізатора шкідливих програм, що виконує ймовірнісне розпізнавання на основі зваженої оцінки ознак, яка використовує поведінковий аналіз на підставі даних, що отримуються від емуляторів, і виконує аналіз за допомогою різних інтелектуальних технологій. Розроблено метод розпізнавання шкідливих програм на основі штучної імунної мережі, що дозволяє підвищити точність і швидкість розпізнавання та виявляти не тільки потенційно шкідливий код, а й не відомі віруси.

Запропоновано модель евристичного аналізатора шкідливих програм на основі штучної нейронної мережі, навчання якої здійснюється за допомогою штучної імунної системи з використанням моделі кодування параметрів, які настроюються, у вигляді адаптивного структурованого мультиантитіла, що призводить до підвищення ефективності її навчання та зменшення кількості нейронів в прихованих шарах.

Розпізнавання шкідливих програм пропонується здійснювати за допомогою мультиагентної системи на основі організації взаємодій як між програмними агентами і файлами, що виконуються, так і програмних агентів між собою, яка дозволяє розпізнавати віруси з мінімально можливими витратами системних ресурсів. Розроблено модель штучної імунної мережі, яка використовується для розпізнавання шкідливих програм, у вигляді мультиагентної системи, що робить її більш узагальненою та дозволяє змінювати параметри і структуру імунної мережі. Проведено експериментальні дослідження та порівняльний аналіз розроблених методів і моделей для різних сімейств вірусів, які показують підвищення ефективності розпізнавання шкідливих програм.

Ключові слова: розпізнавання, шкідлива програма, штучна імунна система, штучна нейронна мережа, мультиагентна систем, мультиантитіло.

АННОТАЦИЯ

Кушнарев М.В. Методы и модели распознавания вредоносных программ на основе искусственных иммунных систем. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.23 – системы и средства искусственного интеллекта. – Харьковский национальный университет радиоэлектроники, Министерство образования и науки Украины, Харьков, 2016.

Диссертационная работа посвящена разработке методов и моделей распознавания вредоносных программ на основе искусственных иммунных систем, что позволяет создавать эффективные системы компьютерной безопасности на основе использования принципов интеллектуальной обработки информации. Предложена обобщенная модель эвристического анализатора вредоносных программ, которая выполняет вероятностное распознавание на основе взвешенной оценки признаков, использует поведенческий анализ на основании данных, получаемых от эмуляторов, и выполняет их интеллектуальный анализ, что позволяет распознавать новые модификации вирусов. Для распознавания вредоносных программ выбран перечень признаков, в качестве которых используются наиболее часто встречающиеся события, связанные с системными вызовами во вредоносных программах, и не встречающиеся в не вредоносных программах.

Предложен метод распознавания вредоносных программ на основе искусственной иммунной сети, которая характеризуется возможностью распознавания не единичным антителом или клоном, а организованной сетью взаимодействующих антител, что позволяет повысить точность и скорость распознавания и обнаруживать не только вредоносный код, но и ранее не известные вирусы. Исследовано влияние иммунных операторов клонирования и мутации антител на скорость сходимости иммунных алгоритмов, используемых для распознавания вредоносных программ. Усовершенствованы подходы к выполнению клонирования и мутации антител для случая вещественного кодирования.

Получил дальнейшее развитие метод распознавания вредоносных программ на основе искусственной нейронной сети, обучение которой предлагается осуществлять с помощью искусственной иммунной системы, использующей модель кодирования настраиваемых параметров в виде адаптивного структурированного мультиантитела. Используется разделение настраиваемых параметров на две независимые части – параметры скрытого слоя и коэффициенты выходного слоя нейронной сети. Размер мультиантитела не является фиксированным, что позволяет уменьшать количество нейронов в скрытых слоях сети.

Для распознавания вредоносных программ предложена мультиагентная система, использующая два вида агентов: агенты-детекторы и агенты-анализаторы. Задача агента-детектора – мониторинг основных уязвимостей операционной системы, и в случае обнаружении аномальной активности – размещение информации о процессе на «доске объявлений». Задача агента-анализатора – исследование процессов, размещенных на «доске объявлений», и принятие решения, какие из них являются потенциальными вирусами и к како-

му классу вредоносных программ они относятся.

Предложено представление модели искусственной иммунной сети, используемой для распознавания вредоносных программ, в виде мультиагентной системы, программные агенты которой идентифицируют исполняемые файлы в сенсорных областях и взаимодействуют между собою в коммуникационных областях, определяемых аффинностями, что обобщает ее описание, делает более гибкой и позволяет изменять параметры и структуру иммунной сети.

Разработана инструментальная среда для моделирования эвристического анализатора вредоносных программ. Проведены экспериментальные исследования и сравнительный анализ разработанных методов и моделей распознавания вредоносных программ с существующими на различных семействах вирусов, которые указали на повышение эффективности их распознавания.

Ключевые слова: распознавание, вредоносная программа, искусственная иммунная система, искусственная нейронная сеть, мультиагентная система, мультиантитело.

ABSTRACT

Kushnaryov M.V. Methods and models of malware recognition based on artificial immune systems. - Manuscript.

Thesis for candidate's degree in engineering science by specialty 05.13.23 – systems and means of artificial intelligence. – Kharkiv National University of Radio Electronics, Kharkiv, Ministry of Education and Science of Ukraine, 2016.

The dissertation is devoted to development of methods and models of malware recognition based on artificial immune systems that allow increasing the efficiency of computer security.

The generalized model of malware heuristic analyzer is proposed. It performs probabilistic recognition based on weighted estimation of features that uses behavioral analysis based on emulator-derived data and analyses it using different intelligent technologies. The method of malicious programs detection is developed using artificial immune network. This method increases the accuracy and speed of recognition and can detect not only potentially malicious code but unknown viruses as well. The model of malware heuristic analyzer based on artificial neural network is proposed. The artificial neural network training is performed by the artificial immune system using the model of adaptive structured multiantibody to encode adjustable parameters of the artificial neural network. It allows not only efficient parameters identifying but also reducing number of neurons in hidden layers. To solve the task of malware recognition the model of artificial immune network is developed. This model is represented in the form of multiagent system to make it more generalized and able to change parameters and structure of the immune network. Experiments and comparative analysis of proposed methods and models are carried for different families of viruses and show the efficiency of the malware recognition.

Keywords: recognition, malware, artificial immune systems, artificial neural network, multi-agent systems, multiantibody.