Адамов Олександр Семенович, старший викладач кафедри автоматизації проектування обчислювальної техніки Харківського національного університету радіо&shy;електроніки: &laquo;Моделі і методи захисту кіберпростору на основі аналізу великих даних з використанням ма&shy;шинного навчання&raquo; (05.13.05 - комп&rsquo;ютерні системи та компоненти). Спецрада Д 64.052.01 у Харківському на&shy;ціональному університеті радіоелектроніки

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Кваліфікаційна наукова праця на правах рукопису

АДАМОВ ОЛЕКСАНДР СЕМЕНОВИЧ

УДК 658:512.011: 681.326: 519.713 **ДИСЕРТАЦІЯ**

МОДЕЛІ І МЕТОДИ ЗАХИСТУ КІБЕРПРОСТОРУ
НА ОСНОВІ АНАЛІЗУ ВЕЛИКИХ ДАНИХ
З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

05.13.05 - комп'ютерні системи та компоненти
Технічні науки

Подається на здобуття наукового ступеня кандидата технічних наук

Дисертація містить результати власних досліджень.

Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело О.С. Адамов

Науковий керівник:

Хаханов Володимир Іванович, доктор технічних наук, професор

Цей примірник дисертації ідентичний за змістом з іншими примірниками, що подані до спеціалізованої вченої ради Д 64.052.01

Учений секретар спеціалізованої вченої ради Д 64.052.01 Є.І. Литвинова

Харків – 2019

**ЗМІСТ**

**ВСТУП 29**

[**РОЗДІЛ 1 ОГЛЯД МОДЕЛЕЙ І МЕТОДІВ ЗАХИСТУ КІБЕРПРОСТОРУ 44**](#bookmark2)

1. **Огляд моделей захисту кіберпростору 44**
2. **Огляд методів захисту кіберпростору 47**
3. [**Детерміністичний підхід 47**](#bookmark3)
4. [**Ймовірнісний підхід та застосування машинного навчання 50**](#bookmark4)
5. [**Атакі на методи машинного навчання 56**](#bookmark5)
6. [**Оцінка методів виявлення кібератак 58**](#bookmark6)
7. [**Аналіз великих даних 60**](#bookmark9)
8. [**Інфраструктура захисту кіберпростору 61**](#bookmark10)
9. [**Висновки до розділу 1 63**](#bookmark11)
10. [**Список використаних джерел до розділу 1 64**](#bookmark12)

**РОЗДІЛ 2 БЛОКЧЕЙН ІНФРАСТРУКТУРА ДЛЯ ЗАХИСТУ КІБЕРСИСТЕМ 72**

1. **Практика використання топ-технологій 72**
2. [**Blockchain Computing 77**](#bookmark13)
3. [**Системні проблеми, пов'язані з «проникненням» і «вразливістю» 91**](#bookmark14)
4. [**Математичний апарат інфраструктури захисного сервісу 95**](#bookmark15)
5. [**Апарат булевих похідних для синтезу тестів 108**](#bookmark18)
6. [**Дедуктивний метод пошуку вразливостей в КС 116**](#bookmark19)
7. [**Висновки до розділу 2 125**](#bookmark22)
8. [**Список використаних джерел до розділу 2 126**](#bookmark23)

[**РОЗДІЛ 3 СИГНАТУРНО-КУБІТНІ МЕТОДИ РОЗПІЗНАВАННЯ ДЕСТРУКТИВНИХ КОДІВ 128**](#bookmark25)

1. [**Вступ. Визначення та правила СSC-комп'ютингу 128**](#bookmark26)
2. [**State of the art. Квантові процеси і явища 135**](#bookmark27)
3. [**Кубітні моделі кіберфізичного соціального СSC-комп'ютингу 138**](#bookmark28)
4. [**Унітарно-кодовані структури даних. Сигнатурний аналіз malware 145**](#bookmark29)
5. [**Метод кубітно-сигнатурного аналізу malware 152**](#bookmark31)
6. [**Модель кубітно-матричного процесора для CSC-компьютінга 159**](#bookmark32)
7. [**^гнатурно-кубітний метод синтезу еталонних логічних схем 161**](#bookmark33)
8. [**Процесорна архітектура CSC-комп'ютингу. Проблема і рішення 163**](#bookmark34)
9. **Висновки до розділу 3 169**
10. [**Список використаних джерел до розділу 3 170**](#bookmark35)

[**РОЗДІЛ 4 МЕТОДИ ДІАГНОСТУВАННЯ КІБЕРАТАК З ВИКОРИСТАННЯМ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ 173**](#bookmark37)

[**4.1 Модель загроз кіберпростору 173**](#bookmark38)

1. [**Проблеми захисту персональних даних і доступу до них 175**](#bookmark39)
2. [**Основні положення кіберпростору 177**](#bookmark40)
3. [**Формальна модель загроз в кіберпросторі 179**](#bookmark41)
4. [**Аналіз великих даних з використанням алгоритмів машинного навчання. 183**](#bookmark42)
5. **Метод атрибутно-орієнтованого впізнання Інтернет посилань з використанням частотних**

**шаблонів 184**

1. [**Формальна модель 186**](#bookmark44)
2. [**Алгоритмічна модель 187**](#bookmark45)
3. [**Метод детектування поліморфних шкідливих програм 190**](#bookmark46)
4. [**Метод пошуку криптопримітивів в троянських програмах-шифрувальниках 200**](#bookmark49)
5. [**Висновки до розділу 4 204**](#bookmark50)
6. [**Список використаних джерел до розділу 4: 205**](#bookmark51)

[**РОЗДІЛ 5 ХМАРНИЙ СЕРВІС ML-АНАЛІЗУ ВЕЛИКИХ ДАНИХ 209**](#bookmark53)

1. [**Архітектура хмарного сервісу 209**](#bookmark54)
2. [**Функціональна модель сервісу 211**](#bookmark55)
3. [**Результати детектування URL-адрес з використанням частотних шаблонів 213**](#bookmark56)
4. **Результати детектування поліморфних шкідливих програм 218**
5. [**Результати пошуку кріптопримітивів в троянські програми-шифрувальники 219**](#bookmark57)
6. [**Висновки до розділу 5 221**](#bookmark58)

**ВИСНОВКИ 224**

**ДОДАТОК А СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАНА ЗА ТЕМОЮ ДИСЕРТАЦІЇ 226**

**ДОДАТОК Б АПРОБАЦІЯ РЕЗУЛЬТАТІВ 231**

**ДОДАТОК В ДОКУМЕНТИ, ЩО ПІДТВЕРДЖУЮТЬ ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ 235 ДОДАТОК Г ПРОГРАМНИЙ ДОДАТОК 239**

**ВСТУП**

В теперішній час спостерігається зростання кількості кібератак на державні і корпоративні (колективні) обчислювальні сервіси. Захищеність цифрової системи визначається захищеністю найбільш уразливого її компонента. Найбільш ефективним способом атак на колективні

обчислювальні системи є пошук уразливого компонента (користувача, програмного або апаратного сервісу) шляхом збору інформації про нього (кіберрозвідку) і запуску атаки на обчислювальну систему за допомогою експлуатації виявленої технічної вразливості або за допомогою методів соціальної інженерії.

Під вразливістю цифрового сервісу, системи або людини слід розуміти несправність або слабкість, використовуючи яку можна навмисно порушити цілісність, доступність і конфіденційність інформації, з якою оперують зазначені суб'єкти.

Сукупність обчислювальних сервісів (C) і оброблюваної інформації (I) окремого суб'єкта (користувача, організації, країни) є кіберпростір (CS) даного суб'єкта:

cs = {C, і} = ц (Ci, Ii), І = [о, N,

де N - кількість цифрових сервісів, які використовуються суб'єктом кіберпростору.

Таким чином, кажучи про захист кіберпростору, слід мати на увазі захист кожного з його сервісів, а також інформації, з якою дані сервіси оперують.

Методи захисту кіберпростору існують як правила захисту, що регламентують процеси доступу користувачів до інформації з обмеженим доступом, і інструментальні засоби: антивіруси, мережеві екрани, системи виявлення і запобігання вторгнень, що використовують інформацію про вже відомі загрози, показують свою неефективність при націлених атаках нульового дня.

Необхідні методи, які дозволять діагностувати атаку невідомого типу або нульового дня (0-day), наприклад, використовуючи евристичні алгоритми або моделювання в віртуальному (хмарному) середовищі з метою виявлення небезпечної поведінки на етапі тестування в демілітаризованій зоні.

Існуючі проблеми захисту кіберпростору:

1. Зростаюча кількість кібератак на кіберпростір.
2. Найбільш ефективними і руйнівними [Stuxnet 2010] є таргінг атаки нульового дня (невідомих на даний момент), які часом не в змозі відбити навіть самі антивірусні компанії.
3. Детерміністичні методи захисту кіберпростору засновані на використанні сигнатур вже відомих кібератак неефективні у разі атак нульового дня.
4. Евристичні методи не мають достатньої точності, що призводить до неприйнятного рівня помилкових спрацьовувань.
5. Поведінкові методи детектують кібератаку вже після її запуску і проникнення за периметр безпеки СК.
6. Методи на основі роботи емуляторів показали свою неефективність через невідповідність реального середовища емульованому, що дозволяє шкідливому коду легко виявляти факт підміни.

Найбільш вагомий внесок в наукові дослідження, що стосуються інформаційної безпеки та захисту від комп’ютерних загроз, внесли вчені: J. von Neumann, L. Penrose, F. Cohen, D.M. Chase, S.R. White, J.O. Kephart, F. Leitold, L. Adleman, B. Schneier, E. Chien, J. Bruce, J. Bates, R. Greenberg, R. Kusnierz, J. Hruska, F. Skulason, J. Norman, E. Spafford, E. Wilding, V. Bontchev, D. Ferbrache, S. Oxley, J. Norstad, S. Emery, M. Smith, K. van Wyk, S. Staniford, Liang-Jie Zhang, Jia Zhang, Hong Cai, Е. Касперский, С. Новиков, Горбенко І.Д, Харченко В.С.

Мета дослідження - істотне зменшення часу виявлення і блокування кібератак, спрямованих на кіберпростір суб'єкта, шляхом використання розроблених матричних моделей і логічних методів тестування, перевірки та діагностування за рахунок введення обчислювальної надмірності в інфраструктуру кіберпростору.

Функція мети (Z) - мінімізація проміжку часу між моментом запуску атаки (A) на кіберпростір і моментом її діагностування (D), протягом якого обчислювальний сервіс залишається скомпрометованим (С), що одночасно дозволяє поліпшити якість сервісу шляхом забезпечення доступності, цілісності і конфіденіційності оброблюваної інформації на період атаки; мінімізації витрат на відновлення працездатності сервісу і фінансових втрат від його простою (TDT) за рахунок введення мінімально необхідної надмірності в інфраструктуру діагностування (I):

Z = F(TDT, TC, I) = min[A(TDT + TC + I)],

де TC - час, на протязі якого обчислювальний сервіс залишається скомпрометованим з моменту запуску атаки зловмисником,

TC = t (D) - t (A),

де t (D) - момент детектування атаки, t (A) - момент запуску атаки.

Задачі дослідження:

1. Удосконалити структурно-логічні моделі і методи перевірки кіберпростору для тестування і діагностування шкідливих компонентів на основі використання дедуктивного аналізу обчислювальних систем.
2. Розробити сигнатурно-кубітні методи синтезу еталонних логічних схем malware-функціональностей і паралельного моделювання malware- driven великих даних для визначення приналежності поточного коду до існуючих деструктивних компонентів в malware бібліотеці.
3. Розробити сигнатурно-кубітну модель активного online cyber se­curity комп'ютингу для моніторингу вхідних потоків malware-даних і управління процесом видалення деструктивних компонентів.
4. Удосконалити засоби захисту кіберпростору шляхом логічного тестування і діагностування атак і шкідливих компонентів на основі використання алгоритмів машинного навчання.
5. Розробити метод атрибутно-орієнтованого розпізнавання URL-адрес з використанням частотних паттернів і метод перевірки поліморфних шкідливих програм на основі врахування контрольних сум Portable Executa­ble секцій в виконувані файли і застосування апарату інтелектуального аналізу даних.
6. Виконати тестування і верифікацію розроблених програмних засобів тестування, перевірки та діагностування шкідливих програм шляхом емуляції атак на основі існуючих malware бібліотек.

Об'єкт дослідження - хмарні і edge-computing технології, засновані на високо-продуктивних дата-центрах, комп'ютерних гаджетах, системах і мережах, виконують сервісні функції зберігання та аналізу великих даних.

Предмет дослідження - структурно-логічні моделі, методи, засоби тестування деструктивних компонентів, захисту індивідуального та колективного сервіс-комп'ютингу від кіберзагроз.

Науково-практична задача - введення в інфраструктуру комп’ютингового простору програмної надмірності в формі моделей, методів і програмних додатків для істотного зменшення часу виявлення і блокування кібератак, спрямованих на кіберпростір суб'єкта, шляхом використання розроблених матричних моделей і логічних методів тестування, перевірки та діагностування.

Сутність дослідження - розробка моделей, методів і програмних додатків для істотного зменшення часу виявлення і блокування кібератак, спрямованих на кіберпростір суб'єкта, шляхом використання розроблених матричних моделей і логічних методів тестування, перевірки та діагностування за рахунок введення обчислювальної надмірності в інфраструктуру кіберпростору.

Методи досліджень подані апаратами: теорії множин і графів, бинарних матриць, інтеллектуального и статистического аналізу даних, мовами об’єктно-орієнтованого програмування - для розробки хмарного віртуального сервіса; прикладна теорія цифрових автоматів, булева алгебра, теорія множин, теорія графів, методи синтезу та аналізу структур даних - для побудови моделей Cyber Security Computing; векторно-логічний аналіз, теорія алгоритмів, мови опису, проектування та моделювання кіберфізичних систем

* для синтезу та аналізу; методи і критерії якості створення комп’ютингових проектів - для тестування і верифікації програмно-апаратних компонентів інфраструктури хмарних сервісів.

**Зв**’**язок роботи з науковими програмами**, **держбюджетними темами**. Розробка теми дисертації здійснювалася відповідно до планів держбюджетних науково-дослідних робіт і міжнародних договорів, виконуваних на кафедрі Автоматизації проектування обчислювальної техніки ХНУРЕ в період з 2007 року, у тому числі: 1) Прикладна держбюджетна НДР № 216 «Енергозберігаючі інформаційні технології на основі паралельних обчислювальних процесів, безпровідних систем і мереж», 2007-2008, № ДР 0107U001540. 2) Договір про дружбу і співробітництво між ХНУРЕ та компанією «Aldec Inc.» (USA) № 04 від 01.11.2011. 3) Фундаментальна держбюджетна НДР № 232 «Теорія й проектування енергозберігаючих цифрових обчислювальних систем на кристалах, що моделюють і підсилюють функціональні можливості людини, 2009-2011, № ДР

0109U001646. 4) Фундаментальна держбюджетна НДР № 269

«Мультипроцесорна система пошуку, розпізнавання та прийняття рішень для інформаційної комп'ютерної екосистеми», 2011-2013, № ДР 0111U002956. 5) Фундаментальна держбюджетна НДР № 258 «Персональний віртуальний кіберкомп'ютер та інфраструктура аналізу кіберпростору», 2012-2014, № ДР 0112U000209. 6) Фундаментальна держбюджетна НДР № 297 “Кіберфізична система - «Розумне хмарне управління транспортом» (Cyber Physical System

* Smart Cloud Traffic Control)”, 2015-2017, № ДР 0115U-000712 від

04.03.2015. 7) Фундаментальна держбюджетна НДР № 316 "Cyber Physical System - Smart Cyber University", 2017-2019, № ДР 0117U0002524. 8) Проект SEIDA BAITSE "Baltic Academic IT Security Exchange", Blekinge Institute of Technology, Sweden; 2011-2014. 9) Проект 530785-TEMPUS-1-2012-1-PL- TEMPUS-JPCR «Curricula Development for New Specialization: Master of Engineering in Microsystems Design (MastMEMS)» сумісно з університетом «Львівська політехніка», Київським національним університетом, Технічним університетом м. Лодзь (Польща), Ліонським університетом (Франція), Університетом м. Ільменау (Німеччина), Університетом м. Павія (Італія), 2012-2016. 10) Проект 544455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR

«Educating the Next Generation Experts in Cyber Security: the new EU- recognized Master’s program (ENGENSEC)», 01 Dec 2013 - 30 Nov 2017.

Автор дисертаційної роботи брав участь при виконанні зазначених договорів і програм як розробник, менеджер і програміст кіберфізичної інфраструктури захисту кіберпростору у вігляді програмних засобів перевірки, діагностування шкідливих програм і атак, що дає можливість виконувати їх моделювання із залученням існуючих додатків і malware бібліотек.

**Наукова новизна результатів досліджень:**

1. Удосконалено структурно-логічні моделі і методи перевірки кіберпростору для тестування і діагностування шкідливих компонентів, які відрізняються використанням методу дедуктивного паралельного аналізу обчислювальної системи для перевірки та діагностування malware.
2. Запропоновано нові методи синтезу еталонних логічних схем mal­ware-функціональностей, які характеризуються використанням сигнатурно- кубітних структур, що дає можливість паралельно моделювати malware- driven великі дані для визначення приналежності поточного коду до існуючих деструктивних компонентів в malware бібліотеці.
3. Розроблено нову модель активного online cyber security комп'ютингу, яка характеризується сигнатурно-кубітним поданням інформації, що дає можливість підвищувати швидкодію процесів моніторингу вхідних потоків malware-даних і управління видаленням деструктивних компонентів.
4. Удосконалено засоби захисту кіберпростору, які відрізняються використанням моделей і методів сигнатурно-логічного тестування атак, пошуку криптопримітивів в троянських програмах-шифрувальниках на основі використання алгоритмів машинного навчання, що дає можливість істотно зменшити час відновлення працездатності обчислювальної структури.

**Практична значимість** результатів досліджень полягає у наступному:

1. Тестуванням, верифікацією і впровадженням розроблених програмних засобів перевірки, діагностування шкідливих програм і атак, що дає можливість виконувати їх моделювання із залученням існуючих додатків і malware бібліотек.
2. Програмною реалізацією методу атрибутного-орієнтованого розпізнавання URL-адрес з використанням частотних паттернів, який відрізняється застосуванням апарату інтелектуального аналізу даних, що дає можливість визначати вірогідну оцінку небезпеки URL-адреси на основі його атрибутів.
3. Програмною реалізацією методу перевірки поліморфних шкідливих програм, який відрізняється інвариантністю до детермінізму сигнатур в коді і урахуванням тільки контрольних сум Portable Executable (PE) секцій в виконуваних файлах, що дає можливість поліпшити продуктивність процедур діагностування деструктивних компонентів.

Отримані в процесі виконання досліджень наукові висновки і практичні результати є достовірними, що підтверджується точністю детектування і класифікацією прикладів загроз нульового дня, серед яких нові версії кріптолокеров і складних загроз (Advanced Persistent Threats - APT); позитивними відгуками вчених і фахівців на доповіді на міжнародних конференціях, присвячених кібербезпеки, таких як Virus Bulletin 2015 Празі, Чехія, 2018 у Монреалі, Канада, OpenStack Summit 2015 Ванкувері, Канада і

OpenStack Summit 2015 Остіні штат Техас, США, IEEE East -West Design & Test Symposium (EWDTS'2017) 2017 в Novy Sad, Serbia.

Результати дисертації у складі моделей, методів та інфраструктури впроваджені у навчальний процес Харківського національного університету радіоелектроніки (акти про впровадження від 20.05.2019, 21.05.2019); у науково-виробничу діяльність компанії Design & Test Lab (довідка від 18.05.2019), у навчальний процес Blekinge Institute of Technology (BTH), Karlskruna, Sweden (лист ‘Statment of Reseach Results Impact on University Ed­ucation Program’ від 29.05.2019).

**Особистий внесок здобувача**. Всі наукові і практичні результати отримані автором особисто. У роботах, опублікованих зі співавторами, здобувачеві належать (аннотації, Додаток А, Б):

1. - мультипроцесорна архітектура для обробки великих даних;
2. - структурна модель malware-аналізу;
3. - модель аналізу інформаційної безпеки кіберпростору;
4. - технології кіберзахисту для корпоративних мереж;
5. - інфраструктура кіберпростору для формування інформаційної безпеки;
6. - удосконалені структурно-логічні моделі і методи перевірки кіберпростору для тестування і діагностування шкідливих компонентів, які відрізняються використанням методу дедуктивного паралельного аналізу обчислювальної системи для перевірки та діагностування malware;
7. - методи синтезу еталонних логічних схем malware- функціональностей для паралельного моделювання malware-driven великих даних; модель активного online cyber security комп'ютингу;
8. - метод визначення поліморфного шпигуна;
9. - метод виявлення URL-адрес за допомогою частотних шаблонів;
10. - аналітична модель оцінки збитків підприємства від шкідливих програм;
11. - модель функціональної перевірки системи на кристалі;
12. - опис програмних засобів для реализації моделей системного

рівня;

1. - модель аналізатора вихідного коду для мов опису апаратури;
2. - метод інтелектуального аналізу даних для функціональної перевірки системи на кристалі;
3. - технологія інтелектуального аналізу даних для функціональної перевірки SoC;
4. - опис та тестування програмних модулів для виявлення троянських включень у програмному забезпеченні;
5. - метод детектування апаратних троянських включень;
6. - методи діагностування і структури даних для інформаційного захисту;
7. - модель захисту індивідуального кіберпростору;
8. - аналіз і тестування програмних модулів;
9. - структурна модель для отримання інформації у великих даних;
10. - модель для захисту кіберпростору в хмарі;
11. - структурна модель криптоперетворення та тестування програмних модулів для операційної системи Android;
12. - метод виявлення таргетованих атак у хмарі;
13. - архітектура безпеки з відкритим кодом для захисту від цільових

атак;

1. - опис програмних засобів для реалізації моделі реагування на хмарні інциденти;
2. - тестування програмних модулів для реалізації методу пом'якшення;
3. - аналіз кібератак;
4. - застосування штучного інтелекту для криптоаналізу;
5. - моделі дескрипторів;
6. - модель пошуку шкідливого коду в програмних продуктах.

**Апробація результатів дисертації**. Результати роботи були

представлені та обговорені на наступних конференціях: IEEE East-West Design and Test Symposium 2007, 2016 (Yerevan, Armenia), 2009 (Moscow, Russia), 2010 (Saint Petersburg, Russia), 2011 (Sevastopol, Ukraine), 2014 (Kyiv, Ukraine), 2015 (Batumi, Georgia), 2017 (Novi Sad, Serbia); International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), 2008 (Lviv-Polyana, Ukraine); Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті», 2012, (Харків, Україна); the 13th International Conference «The Experience of Designing and Application of CAD Systems in Microelectronics», CADSM 2007, 2009, 2015 (Lviv, Ukraine); the Virus Bulletin International Conference, 2015 (Prague, Czech Republic), 2017 (Madrid, Spain), 2018 (Montreal, Canada); OpenStack Summit, 2015 (Vancouver, Canada), 2016 (Austin, TX, USA); Cyber Security Conference UISGCON14, 2018 (Kyiv, Ukraine). Автор також брав участь у конкурсах інноваційних проектів та розробок, як запрошений експерт, спікер, член програмного комітету та журі, серед яких Міжнародна студентська конференція і конкурс наукових робіт з питань інформаційної безпеки «CyberSecurity for the Next Generation», 2011-2014, Kaspersky Lab.

**Публікації**. Результати дисертаційної роботи відображені в 31 друкованій праці: 3 розділи у закордонних монографіях (з них 1 входить до наукометричної бази Scopus), 7 статей (з них 5 - у наукових журналах, включених до «Переліку наукових фахових видань України»; 2 статті в міжнародних наукових журналах за кордоном; 4 статті входять до міжнародних наукометричних баз), а також у 21 міжнародній науковій конференції (з них 13 за кордоном, 12 входять до наукометричної бази Scopus). Здобувач має 13 публікацій у наукометричній базі Scopus та індекс Хірша h=3.

Дисертаційна робота має 241 сторінку (з них 218 представляють основний текст) і містить: 5 розділів, 48 рисунків, 14 таблиць, список джерел з 160 назв (на 16 с.), 4 додатки (на 16 с.), анотації на 27 с.

ВИСНОВКИ

Проведене дослідження вирішує науково-практичну задачу - введення в інфраструктуру комп’ютингового простору програмної надмірності в формі моделей, методів і програмних додатків для істотного зменшення часу виявлення і блокування кібератак, спрямованих на кіберпростір суб'єкта, шляхом використання розроблених матричних моделей і логічних методів тестування, перевірки та діагностування.

Для досягнення поставленої мети - істотного зменшення часу виявлення і блокування кібератак, спрямованих на кіберпростір суб'єкта, шляхом використання розроблених матричних моделей і логічних методів тестування, перевірки та діагностування за рахунок введення обчислювальної надмірності в інфраструктуру кіберпростору, - в роботі були вирішені завдання, які дозволили отримти результати, що мають наукову новизну:

1. *Удосконалені* структурно-логічні моделі і методи перевірки кіберпростору для тестування і діагностування шкідливих компонентів, які відрізняються використанням методу дедуктивного паралельного аналізу обчислювальної системи для перевірки та діагностування malware.
2. *Нові* методи синтезу еталонних логічних схем malware- функціональностей, які характеризуються використанням сигнатурно- кубітних структур, що дає можливість паралельно моделювати malware- driven великі дані для визначення приналежності поточного коду до існуючих деструктивних компонентів в malware бібліотеці.
3. *Нова* модель активного online cyber security комп'ютингу, яка характеризується сигнатурно-кубітним поданням інформації, що дає можливість підвищувати швидкодію процесів моніторингу вхідних потоків malware-даних і управління видаленням деструктивних компонентів.
4. *Нові* методи виявлення кіберзагроз, які здатні навчатися на великих

даних, з метою виявлення кібератак, що можуть бути реалізовані у вигляді Інтернет посилань, поліморфних шкідливих програмах (polymorphic mal­ware), та троянських програмах-шифрувальниках, що займаються здирництвом: метод атрибутно-орієнтованого впізнання Інтернет посилань з використанням частотних шаблонів, що може провести оцінку атрибутів та відрізнити доброякісні, фішинг, та шкідливі посилання; метод детектування поліморфних шкідливих програм, що дозволяє виявляти поліморфні шкідливі програми за допомогою аналізу хешів PE секцій та пошуку схожих секцій у бібліотеці шкідливого коду (після підтвердження детектування PE файла, нові хеші секцій додаються до бібліотеки); метод пошуку криптопримітивів в троянських програмах-шифрувальниках, що дозволяє виявити алгоритми шифрування, використовувані здирником, та можливість дешифрувати зашифровані файли користувача чи організації.

1. *Удосконалені* засоби захисту кіберпростору, які відрізняються використанням моделей і методів сигнатурно-логічного тестування атак, пошуку криптопримітивів в троянських програмах-шифрувальниках на основі використання алгоритмів машинного навчання, що дає можливість істотно зменшити час відновлення працездатності обчислювальної структури.

Практичне значення одержаних результатів досліджень визначається:

1. Тестуванням, верифікацією і впровадженням розроблених програмних засобів перевірки, діагностування шкідливих програм і атак, що дає можливість виконувати їх моделювання із залученням існуючих додатків і malware бібліотек.
2. Програмною реалізацією методу атрибутного-орієнтованого розпізнавання URL-адрес з використанням частотних паттернів, який відрізняється застосуванням апарату інтелектуального аналізу даних, що дає можливість визначати вірогідну оцінку небезпеки URL-адреси на основі його атрибутів.
3. Програмною реалізацією методу перевірки поліморфних шкідливих програм, який відрізняється інвариантністю до детермінізму сигнатур в коді і урахуванням тільки контрольних сум Portable Executable (PE) секцій в виконуваних файлах, що дає можливість поліпшити продуктивність процедур діагностування деструктивних компонентів.