Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет __Комп'ютерної інженерії та управління_____
(повна назва)
Кафедра Автоматизації проектування обчислювальної техніки
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти____перший (бакалаврський)_____
(рівень вищої освіти)

Архітектура спеціалізованого процесора для розпізнавання шкідливих загроз
(тема)

Виконав: здобувач IV курсу, групи КІУКІ-21-8
_____Нестеренко М. І._____
(прізвище, ініціали)
Спеціальність *123 _ Комп'ютерна інженерія*
Тип програми ____освітньо-професійна_____
(освітньо-професійна або освітньо-наукова)
Освітня програма_____
Комп'ютерна інженерія _____
(повна назва освітньої програми)

Керівник Хаханов В.І.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри АПОТ _____ Чумаченко С.В
(підпис) (прізвище, ініціали)

2025 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління

Кафедра Автоматизації проектування обчислювальної техніки

Рівень вищої освіти перший (бакалаврський)

Спеціальність 123_Комп'ютерна інженерія
(шифр і назва)

Тип програми Освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Комп'ютерна інженерія
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри АПОТ
Чумаченко С.В.
(підпис)
« 06 » 05 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Нестеренку Максиму Ігоровичу
(прізвище, ім'я, по батькові)

1. Тема роботи (проекту) Архітектура спеціалізованого процесора для розпізнавання шкідливих загроз
затверджена наказом по університету від " 21 " 05 2025 р. № 403 Ст.
2. Термін подання студентом роботи до екзаменаційної комісії 17.06.2025
3. Вихідні дані до роботи (проекту)
Моделі, метрики, архітектури комп'ютингу кіберзахисту

4. Зміст пояснювальної записки (перелік питань, що підлягають розробці):
Огляд технологій та публікацій
Аналіз моделей, методів, метрик, технологій комп'ютингу кіберзахисту
Розробка архітектури спеціалізованого процесору для паралельного моделювання та розпізнавання шкідливих загроз у потоках великих даних.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів)

__14__ слайд_____

6. Консультанти розділів роботи (проекту)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи (проекту)	Термін виконання етапів проекту (роботи)	Примітка
1	Видача теми проекту, узгодження і затвердження	06.05.2025 - 06.05.2025	
2	Аналіз проблемної галузі, постановка задачі, вибір інструментальних засобів. Складання аналітичного огляду стану технологій. Аналіз останніх досліджень та публікацій.	07.05.2025 -10.05.2025	
3	Опис обраних моделей, методів та алгоритмів	10.05.2025 -17.05.2025	
4	Розробка архітектури спецпроцесору	18.05.2025 -30.05.2025	
5	Розробка алгоритму	01.06.2025 -05.06.2025	
6	Оформлення пояснювальної записки	06.06.2025 -10.06.2025	
7	Перевірка виконаного проекту керівником,	11.06.2025 -12.06.2025	
8	Захист проекту	23.06.2025	

Дата видачі завдання 06.05.2025

Здобувач _____ _____ Нестеренко М. І.
(підпис)

Керівник роботи _____ проф. Хаханов В.І.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 50 с., 6 рисунків, 1 дод., 14 джерел.

СИСТЕМА, АРХІТЕКТУРА, СЕРВІС, КОМП’ЮТИНГ, КІБЕРЗАХИСТ, МЕТРИКА, ПРОЦЕССОР

Тематика роботи стосується питань створення архітектури спеціалізованого процесору для паралельного моделювання та розпізнавання шкідливих загроз у потоках великих даних на основі моделей, метрик та технологій комп’ютингу кіберзахисту.

В роботі розглянуто стан технологій; аналіз сучасних публікацій, актуальні моделі, методи, метрики та технології комп’ютингу кіберзахисту, розробка архітектури спеціалізованого процесору для паралельного моделювання та розпізнавання шкідливих загроз у потоках великих даних.

ABSTRACT

Bachelor’s thesis contains 50 pages format A4, 6 figures, 1 application, 14 sources.

SYSTEM, ARCHITECTURE, SERVICE, COMPUTING, CYBER DEFENSE, METRICS, PROCESSOR

The work focuses on developing a specialized processor architecture for the parallel modeling and recognition of malicious threats within large data streams. This is based on various models, metrics, and technologies pertaining to cybersecurity.

The study reviews the current state of the field, analyzes modern publications, and examines contemporary models, methods, metrics, and technologies in cybersecurity computing. It aims to create a processor architecture specifically designed for effectively handling the challenges of modeling and identifying threats in vast amounts of data.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

AI – Artificial Intelligence (штучний інтелект);

CSC – Cyber Security Computing (комп’ютинг кіберзахисту);

GDPR – Загальний регламент захисту даних;

GenAI – Generative AI (генеративний ШІ);

IAM – Identity and Access Management (управління ідентифікацією та доступом);

IoT – Internet of Things;

LLM – Large Language Models (великі мовні моделі);

LV – значення змінної;

ML – Логічний malware-елемент;

MF – Malware-функціональність;

MV – Malware-змінна;

SBCP – Security Behavior and Culture Program (програма формування культури поведінки та безпеки;

SRM – Supplier Relationship Management (управління взаєминами з постачальниками);

ІБ – інформаційна безпека;

ШІ – штучний інтелект.

ВСТУП

Тематика роботи стосується питань створення архітектури спеціалізованого процесору для паралельного моделювання та розпізнавання шкідливих загроз у потоках великих даних на основі моделей, метрик та технологій комп’ютингу кіберзахисту.

Задачі: огляд стану технологій; аналіз сучасних публікацій, актуальні моделі, методи, метрики та технології комп’ютингу кіберзахисту, розробка архітектури спеціалізованого процесору для паралельного моделювання та розпізнавання шкідливих загроз у потоках великих даних.

Мета роботи – розробка архітектури спеціалізованого процесора для паралельного моделювання та розпізнавання шкідливих загроз у потоках великих даних на основі математичного та технологічного апарату комп’ютингу кіберзахисту.

1 СТАН ТЕХНОЛОГІЙ

Аналізується стан сучасних технологій на основі прогнозів консалтингової компанії Gartner для трендів у сфері кібербезпеки на 2025 рік. Наводиться огляд літератури.

1.1 Топ тренди кібербезпеки Gartner 2025

Gartner представив [1] головні тренди у сфері кібербезпеки на 2025 рік. Вони зумовлені розвитком генеративного ШІ, цифровою децентралізацією, взаємозалежністю ланцюжків поставок, зміною регуляторних вимог, повсюдною нестачею фахівців та ландшафтом загроз, що постійно змінюється.

«Керівники служб кібербезпеки та управління ризиками (SRM) стикаються з цілим рядом труднощів та можливостей у своєму прагненні здійснити перетворення та забезпечити стійкість. Їхні зусилля в обох напрямках повинні не тільки підтримати інновації, але й забезпечити захищеність і стійкість у цифровому світі, що швидко змінюється», – пише у прес-релізі Алекс Майклс (Alex Michaels), старший головний аналітик Gartner [1].

Gartner виділив шість трендів, які надаватиме великий вплив у сфері інформаційної безпеки (ІБ):

1. GenAI трансформує програми захисту даних. Більшість зусиль та фінансових ресурсів SRM зазвичай націлені на захист структурованих даних, насамперед баз даних, але прихід генеративного ШІ зміщує приціл на захист неструктурованих даних: тексту, зображень та відео. «Багато керівників SRM повністю переорієнтували свою стратегію інвестицій, що суттєво вплинуло на процеси навчання, розгортання даних та інференсу великих мовних моделей (LLM), – пише Майклс. – Зрештою, це зрушення підкреслює мінливі пріоритети, які повинні взяти до уваги керівники SRM, говорячи про вплив GenAI на свої програми» [1].

2. Управління машинними ідентифікаційними даними. Впровадження GenAI, хмарних сервісів, автоматизації та практики DevOps привело до широкого використання машинних акаунтів і облікових даних для фізичних пристроїв і робочих навантажень. Без належного контролю це може значно збільшити поверхню атаки у компаній.

Для захисту від атак керівникам SRM необхідно виробити та впровадити надійну стратегію управління ідентифікацією та доступом (IAM – Identity and Access Management) пристроїв, і це мають бути скоординовані зусилля у масштабах усієї організації. Опитування 335 керівників IAM по всьому світу, проведене у серпні-жовтні 2024 року, показало, що служби IAM контролюють лише 44% машинних ідентифікаторів у своїй компанії.

3. «Тактичний» ШІ. Керівники SRM спостерігають неоднозначні результати впровадження ШІ; це змушує їх переглянути пріоритети своїх ініціатив, зосередившись на вужчих сценаріях використання з безпосередньою віддачею. При такому тактичному впровадженні методи та інструменти ШІ будуть пов'язані з існуючими показниками та ініціативами, дозволяючи більш наочно продемонструвати реальну цінність інвестицій у ШІ. «Зараз на керівників SRM покладено пряму відповідальність забезпечити безпеку використання інструментів ШІ третіми особами, захистити корпоративні ШІ-додатки та підвищити кібербезпеку за допомогою ШІ, – пише Майклс. – Зосередившись на тактичних, відчутно корисних поліпшеннях, вони зможуть мінімізувати ризики для своїх програм» [1].

4. Оптимізація технологій кібербезпеки. Як показало опитування 162 великих компаній у серпні-жовтні минулого року, вони використовують у середньому 45 інструментів кібербезпеки. Маючи вибір із понад 3000 вендорів ІБ (інформаційної безпеки), керівники SRM повинні оптимізувати свій інструментарій, щоб створити більш ефективну та дієву програму кібербезпеки.

Gartner рекомендує прагнути до балансу, який влаштовує закупівель, архітекторів/інженерів безпеки та інші зацікавлені сторони, щоб забезпечити

належний рівень захищеності. Для цього потрібно консолідувати та відтестувати основні елементи управління безпекою та вибудовувати архітектуру, яка підвищує переносимість даних. Моделювання кіберзагроз та технологічні драйвери, такі як впровадження ШІ, також можуть бути використані для оцінки потреб у передових технологіях.

5. Зростаюча важливість культури поведінки у безпеці. Програми формування культури поведінки та безпеки (SBCP – Security Behavior and Culture Program) досягли переломного моменту більшості організацій. Успішні керівники SRM визнають цінність цих програм підвищення рівня кібербезпеки. За прогнозом Gartner, одним із головних драйверів змін у цих програмах є генеративний ШІ: до 2026 року компанії, що поєднують цю технологію з інтегрованою архітектурою на базі платформ у своїх програмах SBCP, матимуть на 40% менше ІБ-інцидентів, викликаних співробітниками.

Цей тренд набирає сили з огляду на зростання визнання того, що не тільки небезпечна, а й правильна поведінка людини є важливою складовою кібербезпеки. Як результат, заходи, спрямовані на культуру та поведінку, стали дієвим підходом до вирішення проблеми усвідомлення кібер-ризиків та відповідальності за них на людському рівні. Це відбиває стратегічний зрушення запровадження безпеки у корпоративну культуру.

6. Боротьба із вигорянням. Вигоряння керівників SRM та їх команд є гострою проблемою в галузі, яка вже страждає від системної нестачі кадрів. Цей непереборний стрес виникає через нестримно зростаючі вимоги забезпечити захищеність все більш складних організацій в умовах постійно мінливих загроз, нормативного та ділового середовища, при обмежених повноваженнях, підтримці керівництва та ресурсах. «Потрібно розпізнавати та усувати вигоряння команд, щоб досягти ефективності програм кібербезпеки, – наголошує Майклс. – Успішні керівники SRM приділяють першорядну увагу не лише боротьбі з власним стресом, а й запроваджуючи загальнокомандні програми благополуччя, які реально підвищують особисту стійкість до стресів кожного» [1].

1.2 Тенденції в галузі кібербезпеки та інноваційні способи боротьби

Кібербезпека розвивається стрімкими темпами: хакери та постачальники послуг безпеки безперервно змагаються, намагаючись обійти один одного, постійно виникають нові загрози та інноваційні способи боротьби з ними.

1. Ризики кібербезпеки під час віддаленої роботи. Пандемія Covid-19 змусила більшість організацій перевести співробітників на віддалену роботу, часто досить стислі терміни. Багато досліджень показують, що після пандемії більшість співробітників продовжить працювати віддалено. Робота вдома створює нові ризики і є однією з найбільш обговорюваних тенденцій у сфері кібербезпеки. Захист домашніх офісів, як правило, набагато нижчий, ніж централізованих, які зазвичай оснащені мережевими екранами та маршрутизаторами, а керування доступами регулюється групою IT-безпеки. Перехід на віддалену роботу здійснювався поспіхом, щоб не порушувати робочі процеси, і перевірка безпеки могла виконуватися менш суворо, ніж зазвичай. Цим можуть скористатися кіберзлочинці.

Багато співробітників використовують особисті пристрої для двофакторної аутентифікації, і вони можуть використовувати мобільні версії додатків для обміну миттєвими повідомленнями, такі як Microsoft Teams і Zoom. Розмиття кордонів між особистим та професійним життям збільшує ризик потрапляння конфіденційної інформації в чужі руки.

Отже, важливий тренд кібербезпеки – привернути увагу компаній до проблем безпеки, що виникли в результаті переходу на віддалену роботу: виявлення та усунення нових уразливостей систем безпеки, покращення систем, впровадження заходів безпеки та забезпечення належного моніторингу та документації.

2. Розвиток Інтернету речей. Розвиток інтернету речей створює нові можливості для кіберзлочинців. Інтернет речей відноситься до фізичних

пристроїв, відмінних від комп'ютерів, телефонів та серверів, які підключаються до інтернету та обмінюються даними. Приклади таких пристроїв – фітнес-трекери, розумні холодильники, розумні годинники та голосові помічники, такі як Amazon Echo та Google Home. За оцінками, до 2026 року у світі буде встановлено 64 мільярди пристроїв інтернету речей. Тенденція до віддаленої роботи сприяє збільшенню їхньої кількості.

Велика кількість додаткових пристроїв змінює динаміку та поверхню кібератаки – збільшується кількість потенційних точок входу для зловмисників. У порівнянні з ноутбуками та смартфонами, пристрої інтернету речей мають менше можливостей для обробки та зберігання даних. Це ускладнює використання мережевих екранів, антивірусу та інших програм безпеки для їх захисту. Атаки на інтернет речей – це найбільш обговорюваний тренд у сфері кібербезпеки.

3. Зростання кількості програм-вимагачів. Програми-здирники – це не нова загроза, вони існують вже близько двох десятиліть, і зростання їхньої кількості продовжується. За оцінками, нині існує понад 120 сімейств програм-вимагачів, а зловмисники досконало опанували мистецтво приховування шкідливого коду. Програми-вимагачі – це простий для зловмисників спосіб отримати фінансову вигоду, що частково пояснює зростання їхньої кількості. Ще одним фактором стала пандемія Covid-19. У багатьох організаціях прискорений перехід до цифрових технологій у поєднанні з віддаленою роботою спричинив нові атаки програм-вимагачів. В результаті збільшилася кількість атак, так і розмір необхідного викупу.

Під час атаки зловмисники крадуть дані компанії, а потім шифрують їх, щоб компанія не могла отримати доступ до них. Після цього кіберзлочинці шантажують компанію розкриттям конфіденційних даних, якщо не буде сплачено викуп. Такі атаки завдають відчутних збитків з огляду на конфіденційність даних, а також економічні наслідки сплати викупу.

У 2020 році програми-здирники увійшли в історію, як причина першої зареєстрованої смерті в результаті кібератаки. У процесі атаки на лікарню в

Німеччині було заблоковано доступ до систем, що унеможливило лікування пацієнтів. В результаті жінка, яка потребує невідкладної допомоги, була доставлена до сусідньої лікарні на відстані 20 миль, але не вижила.

Фішингові атаки здирників стають все більш витонченими за рахунок машинного навчання та більш організованого обміну. Зловмисники зазвичай вимагають викупу в криптовалюті, яку важко відстежити. Найближчим часом очікуються нові атаки програм-вимагачів на організації, які не використовують надійну систему кібербезпеки.

4. Збільшення кількості хмарних сервісів та загроз безпеці хмарної інфраструктури. Вразливість хмарної інфраструктури залишається однією з основних тенденцій кібербезпеки. Швидкий повсюдний перехід до віддаленої роботи під час пандемії різко збільшив потребу у хмарних сервісах та інфраструктурі, що позначилося на безпеці організацій.

Хмарні послуги мають ряд переваг: масштабованість, ефективність та економія коштів, але водночас є основною метою для зловмисників. Неправильно налаштовані параметри хмарних сервісів можуть стати причиною витоку даних, несанкціонованого доступу, небезпечних інтерфейсів та злому облікових записів. Середня ціна витоку даних становить 3,86 мільйона доларів, тому організаціям необхідно вжити заходів щодо мінімізації хмарних загроз.

Крім витоку даних, організації стикаються з наступними проблемами мережевої та хмарної безпеки: забезпечення відповідності нормативним вимогам у різних юрисдикціях, забезпечення достатнього досвіду в IT для задоволення вимог хмарних обчислень;

Внутрішні загрози, як випадкові, так і навмисні, викликані несанкціонованим віддаленим доступом, ненадійними паролями, незахищеними мережами та неправомірним використанням особистих пристроїв.

5. «Розумні» атаки соціальної інженерії. Атаки соціальної інженерії, такі як фішинг, не є новими, але становлять серйозні загрози в умовах

віддаленої роботи, що широко поширилася останнім часом. Зловмисники націлені на співробітників, які підключаються до мережі роботодавця з дому, оскільки вони є найлегшими жертвами.

Зростання використання таких програм для обміну повідомленнями, як WhatsApp, Slack, Skype, Signal, WeChat спричинило зростання популярності SMS-фішингу (змішинг). Зловмисники використовують ці платформи, щоб змусити користувачів завантажити шкідливі програми на свої телефони.

Існує також голосовий фішинг (вішинг, від "voice phishing"), який здобув популярність після злому Twitter у 2020 році. Хакери втілювалися співробітниками IT-відділу, дзвонили представникам служби підтримки клієнтів і обманом змушували їх надати доступ до важливих внутрішніх інструментів. Голосовий фішинг використовувався в атаках на багато компаній, включаючи фінансові установи та великі корпорації.

Крім того, використовується підміна SIM-картки – вид шахрайства, коли зловмисники пов'язуються з представниками мобільного оператора конкретного клієнта та переконують їх, що SIM-картка зламана. Це призводить до необхідності перенесення номера телефону на іншу картку. Якщо обман виявиться успішним, кіберзлочинці матимуть доступ до цифрового вмісту телефону жертви.

Організації посилюють захист від фішингу, а зловмисники постійно шукають нові способи бути на крок попереду: наприклад, використовують витончені набори для фішингу, які атакують жертв залежно від їхнього розташування.

6. Конфіденційність даних як дисципліна. Однією з ключових тенденцій у сфері безпеки даних є виділення конфіденційності даних у самостійний напрямок. Численні гучні кібератаки призвели до розкриття мільйонів записів ідентифікаційної інформації. Поряд з цим, у світі приймаються суворіші закони про захист даних, такі як Загальний регламент захисту даних (GDPR), прийнятий у Євросоюзі, що свідчить про зростання пріоритету конфіденційності даних.

Організації, які не дотримуються нормативних вимог та не відповідають очікуванням споживачів, ризикують отримати штрафи, заробити негативну репутацію та втратити довіру клієнтів. Конфіденційність даних впливає на всі аспекти діяльності організації. В результаті організації приділяють більше уваги питанням конфіденційності даних: забезпечення контролю доступу на основі ролей, багатофакторної аутентифікації, шифрування даних при передачі та зберіганні, сегментації мережі та зовнішніх оцінок для виявлення областей, що потребують покращення.

7. Удосконалення багатофакторної автентифікації. Багатофакторна автентифікація вважається золотим стандартом автентифікації. Однак зловмисники знаходять нові способи її обходу, зокрема аутентифікації за допомогою SMS або телефонного дзвінка. У 2020 році Microsoft рекомендував користувачам припинити використання багатофакторної аутентифікації по телефону, а замість цього використовувати аутентифікатори на основі програм та ключі безпеки.

SMS-повідомлення мають деякий вбудований захист, але повідомлення, що надсилаються, у тому числі для цілей автентифікації, не зашифровані. Це означає, що зловмисники можуть виконувати автоматичні атаки типу "людина посередині" для отримання одноразових текстових паролів. Це вразливість, зокрема, для онлайн-банкінгу, де аутентифікація часто виконується за допомогою SMS. Для вирішення цієї проблеми банки та інші організації все частіше намагаються використовувати багатофакторну автентифікацію на основі програм: Google Authenticator, Authy та інших.

8. Активне зростання штучного інтелекту. Кількість загроз кібербезпеці занадто велика, і люди не можуть впоратися з ними поодинці. В результаті організації все частіше звертаються до штучного інтелекту та машинного навчання з метою оптимізації інфраструктури безпеки. Це дозволяє знизити втрати: постраждалі від витоку даних організації, які повністю розгорнули технологію штучного інтелекту, заощадили в середньому 3,58 мільйона доларів у 2020 році.

Штучний інтелект відіграє першорядну роль у створенні автоматизованих систем безпеки, обробці природної мови, розпізнаванні осіб та автоматичному виявленні загроз. Він також дозволяє з високою швидкістю аналізувати величезні обсяги даних ризиків. Це вигідно як для великих компаній, що працюють з великими обсягами даних, так і для малих та середніх компаній, групи безпеки яких можуть відчувати брак ресурсів.

Штучний інтелект надає компаніям широкі можливості для більш ефективного виявлення загроз, проте зловмисники також застосовують його для автоматизації атак, використовуючи методи спотворення даних та крадіжки моделей.

Продовжується розвиток сфер практичного застосування штучного інтелекту. Очікується, що складність та функції інструментів безпеки, заснованих на штучному інтелекті та машинному навчанні, ще вдосконалюватимуться.

9. Мобільна кібербезпека виходить на перший план. Перехід до віддаленої роботи прискорює зростання використання мобільних пристроїв. Співробітники, які працюють віддалено, часто використовують різноманітні мобільні пристрої, планшети та телефони, підключені до загальнодоступних мереж Wi-Fi, а також інструменти для віддаленої спільної роботи. В результаті продовжується зростання та розвиток мобільних загроз. Розгортання технології 5G, що продовжується, також є потенційним джерелом уразливостей у системі безпеки, які необхідно буде усунути відразу після виявлення.

Мобільні загрози включають такі: спеціалізоване шпигунське програмне забезпечення для стеження за програмами для обміну зашифрованими повідомленнями; використання критичних уразливостей безпеки на пристроях Android; мобільне шкідливе програмне забезпечення з різними можливими сценаріями застосування, від розподілених атак типу «відмова в обслуговуванні» (DDoS) до SMS-спаму та крадіжки даних.

1.3 Аналіз літератури

Квантові технології паралельних обчислень ефективно використовуються для вирішення комбінаторних проблем, емулюючи обчислення на класичних комп'ютерах [4-6].

Квантові обчислення та інформація – це нова, швидко розвиваюча міждисциплінарна галузь. Тому нелегко зрозуміти її фундаментальні концепції та основні результати, не зіткнувшись із численними технічними деталями. Книга [4] є корисним та не надто складним посібником для читача. Вона пропонує простий та самостійний вступ; попередні знання квантової механіки чи класичних обчислень не потрібні. Її можна розглядати як підручник для односеместрового вступного курсу з квантової інформації та обчислень як для здобувачів освіти старших курсів бакалаврату, так і для аспірантів. Він містить велику кількість розв'язаних вправ, які є важливим доповненням до тексту, оскільки допоможуть студенту ознайомитися з предметом. Висвітлено фундаментальні принципи квантової інформації та обчислень і які мають базові знання, отримані на бакалаврському курсі з фізики, математики чи інформатики.

Книга [5] є збіркою оглядів вибраних тем квантової інформації. Колись квантовий ефект розглядався як перешкода для належної обробки інформації в існуючих інформаційних системах. Нещодавно було виявлено, що квантові ефекти, навпаки, дуже корисні як ресурс, що використовується в обробці інформації. Ця галузь досліджень називається квантовою інформацією і швидко розвивається як нова парадигма для інформаційних систем. Наприклад, можна швидко факторизувати велике число за допомогою алгоритму Шора на квантовому комп'ютері, коли квантовий комп'ютер стане доступним, і можна безпечно спілкуватися без будь-яких припущень щодо складності обчислень, використовуючи квантовий розподіл ключів. Ці протоколи квантової інформації неможливо реалізувати без квантових ефектів. У дослідженні існуючих інформаційних процесів можна вивчати

апаратне та програмне забезпечення окремо, оскільки їхні ролі чітко розділені. Однак таке розділення між ними стає перешкодою для всього дослідження квантової інформації. Для розробки квантових алгоритмів і протоколів необхідно розуміти математичний опис квантових явищ. Реалізація квантових інформаційних систем вимагає розробки квантових пристроїв, для чого потрібно розуміти теоретичну схему квантової інформатики.

Одна з найбільш цитованих книг з фізики всіх часів [6] залишається найкращим підручником у цій захопливій галузі науки. У цьому вичерпному підручнику описано такі визначні ефекти, як швидкі квантові алгоритми, квантова телепортація, квантова криптографія та квантова корекція помилок. Пояснюється, що таке квантовий комп'ютер, як його можна використовувати для вирішення проблем швидше, ніж «класичні» комп'ютери, та його реальної реалізації. Підручник завершується поглибленим розглядом квантової інформації.

Таблиці істинності або кубічні покриття для опису логічних елементів є ефективними структурами даних для вирішення проблем CSC-комп'ютингу та пошуку необхідних даних [7, 8].

Відома книга [7] пропонує ґрунтовне дослідження тестування та проектування цифрових систем, з акцентом на практичних застосуваннях та методологіях моделювання. Вона структурована на п'ятнадцять розділів, що охоплюють різні концепції тестування, такі як методології сканування та архітектури BIST, хоча деякі теми, такі як перекриття несправностей, висвітлені в ній менше. Надається глибоке розуміння сучасних технологій тестування, але не містить деталей на рівні схем.

У [8] запропоновано нову технологію синтезу та аналізу векторно-керованої логічної схеми (гейт- та RTL-логіки) на основі метрики тестового рівняння, яка формує xor-зв'язки між тестом, функцією та несправностями. Представлено векторну форму для опису структур, яка дозволяє застосовувати розроблені вченими технології синтезу та аналізу тестів

логічних схем для ефективного вирішення задач тестування графових структур та моделей автоматів цифрових пристроїв. Основні задачі технічної діагностики (синтез тестів, розробка моделей пристроїв, аналіз несправностей) визначаються як похідні від відношень тестового рівняння. Введено поняття Х-функції для вимірювання всіх процесів та явищ у цифровому світі; це функція, яку неможливо модифікувати та/або мінімізувати. Представлено метод синтезу кубіт-векторних тестів на основі похідних, обчислених за допомогою векторного покриття логіки. Наведено оцінки обчислювальної складності синтезу тестів та дедуктивні формули для логіки та їх використання в моделюванні несправностей.

Автоматичний синтез кубітних покриттів функціональностей є одним з основних важко формалізованих завдань, без якої неможливо виконувати аналітику великих даних [9-13].

Монографія [9] представляє кіберкультуру мікро-, макро-, космологічних та віртуальних обчислень. Книга показує, як вони працюють для формулювання, пояснення та прогнозування сучасних процесів і явищ, що використовуються для моніторингу та керування технологіями у фізичному та віртуальному просторі. Висувається базова пропозиція щодо перетворення опису таблиці істинності функцій та матриці суміжності структури на вектор кубітів, який зосереджений на обчисленнях, керованих пам'яттю, на основі логічних паралельних операцій. Автори пропонують метрику для вимірювання процесів та явищ у кіберпросторі, а також архітектуру логічних асоціативних обчислень для прийняття рішень та аналізу великих даних. Книга окреслює інноваційну теорію та практику проектування, тестування, моделювання та діагностики цифрових систем на основі використання вектору покриття кубітів для опису функціональних компонентів та структур. Автори надають опис технології діагностики HDL-моделі SoC на основі Test Assertion Blocks Activated Graph. Запропоновано приклади кіберфізичних систем для цифрового моніторингу та хмарного управління соціальними об'єктами та транспортом. Представлена автоматна

модель космологічних обчислень пояснює циклічну та гармонійну еволюцію матерійно-енергетичної сутності, а також просторово-часову форму Всесвіту.

В [10] запропоновано одне з можливих рішень проблеми створення та тестування теорії та методів квантових обчислень, керованих пам'яттю, на класичних комп'ютерах для їх подальшого застосування в усіх сферах людської діяльності. Використовуються інженерно-орієнтовані визначення типів обчислень, включаючи квантові, включаючи поняття суперпозиції та заплутаності, а також обчислення, керовані пам'яттю. Пояснюється необхідність спільного та паралельного вирішення проблеми створення ринково доступного квантового комп'ютера та розробки квантово-орієнтованих додатків і хмарних сервісів. Представлено приклади квантового проектування та тестування фрагментів цифрових схем, керованих пам'яттю. Запропоновано метод синтезу та мінімізації тестів функціональності "чорної скриньки", що використовує матрицю похідних кубітів та секвенсор для визначення квазіоптимального покриття.

У [11] запропоновано кубітни моделі та методи покращення продуктивності програмного та апаратного забезпечення для аналізу цифрових пристроїв шляхом збільшення розмірності структур даних та пам'яті. Введено основні поняття, термінологію та визначення, необхідні для реалізації квантових обчислень під час аналізу віртуальних комп'ютерів. Представлено результати дослідження щодо проектування та моделювання комп'ютерних систем у кіберпросторі на основі використання двокомпонентної структури <пам'ять – транзакції>.

У [12] запропоновано інфраструктуру для паралельного аналізу великих даних з метою пошуку, розпізнавання образів та прийняття рішень, що базується на використанні булевої метрики вимірювання кіберпростору. Вона характеризується використанням лише логічної операції xor для визначення кібервідстані шляхом циклічного замикання принаймні одного об'єкта, що дозволяє значно збільшити швидкість аналізу великих даних. Запропоновано новий підхід до векторно-логічної обробки великих даних,

заснований на повному виключенні арифметичних операцій, які впливають на продуктивність та апаратну складність, який може бути ефективно реалізований на основі сучасних багатопроцесорних цифрових систем-на-чіпах та віртуальних паралельних процесорів, що працюють під керуванням кіберфізичних систем або хмарних сервіс-фільтрів. Запропоновано кубітно-векторну модель обчислювального автомата, яка характеризується транзакційною взаємодією компонентів пам'яті, що представляють собою комбінаційні та послідовні елементи та реалізовані у вигляді кубіта або "квантових" примітивів, необхідних для створення паралельних віртуальних комп'ютерів та хмарно-орієнтованих процесорів. Розроблено нову структурну модель аналізу великих даних, яка характеризується використанням хмарних сервісів, кіберфізичних та пошукових систем, віртуальних паралельних мультипроцесорів з мінімальним набором векторно-логічних операцій для точного пошуку інформації на основі запропонованої булевої метрики та нечислових критеріїв якості, що дозволяє створити семантичну інфраструктуру кіберпростору шляхом класифікації компетенцій та метричного впорядкування великих даних по всій кіберекосистемі планети.

У [13] запропоновано хмарний сервіс QuaSim, призначений для моделювання та верифікації цифрових систем на основі транзакцій між адресованими компонентами пам'яті для реалізації будь-якої функціональності. Описано новий підхід до синтезу та аналізу цифрових систем з використанням векторної форми (квантової) для визначення комбінаційних та послідовних структур для їх реалізації в елементах пам'яті; він суттєво відрізняється від класичної теорії проектування дискретних пристроїв на основі таблиць істинності компонентів. Квантові або кубітні структури даних використовуються для реалізації обчислювальних процесів з метою підвищення продуктивності аналізу цифрових систем та зменшення обсягу пам'яті шляхом унарного кодування станів вхідних, внутрішніх та вихідних змінних, а також реалізації кубітних векторів в елементах пам'яті

FPGA, які реалізують комбінаційні та послідовні примітиви. Впровадження квантових моделей, що базуються лише на пам'яті, для опису цифрових компонентів у практиці проектування комп'ютерних систем безпосередньо впливає на збільшення виходу продукції, дозволяє підвищити надійність комп'ютерної продукції, знизити вартість проектування та виробництва, а також забезпечити автономний дистанційний та онлайн-ремонт без участі людини.

1.4 Висновки та постановка завдання

Проаналізовано технологічні тенденції у сфері кібербезпеки, що визначені компанією Gartner на 2025 рік. Вони зумовлені розвитком генеративного ШІ, цифровою децентралізацією, взаємозалежністю ланцюжків поставок, зміною регуляторних вимог, повсюдною нестачею фахівців та ландшафтом загроз, що постійно змінюється. Мобільна **к**ібербезпека – це широка сфера, що включає інші області: внутрішня та хмарна безпека, мережна безпека, а також безпека мереж, що складаються з великої кількості підключених об'єктів (наприклад, інтернет речей), таких як пристрої, що носяться, та автомобільні. Немає єдиного методу захисту додатків у небезпечних середовищах. Для підвищення загальної безпеки використовують додаткові рівні безпеки. Фахівці безпеки спираються на поєднання захисту програмного забезпечення для мобільних пристроїв з апаратними рішеннями безпеки для підвищення надійності зберігання конфіденційних даних. Апаратні рішення, як розробка спецпроцесорів кіберзахисту, становлять предмет для дослідження, розвитку та впровадження комп’ютерними інженерами.

Мета роботи – розробка архітектури спеціалізованого процесора для паралельного моделювання та розпізнавання шкідливих загроз у потоках великих даних на основі математичного та технологічного апарату комп’ютингу кіберзахисту.

Задачі: огляд стану технологій; аналіз сучасних публікацій, актуальні моделі, методи, метрики та технології комп’ютингу кіберзахисту, розробка архітектури спеціалізованого процесору для паралельного моделювання та розпізнавання шкідливих загроз у потоках великих даних

2 МОДЕЛІ, МЕТОДИ, МЕТРИКИ, ТЕХНОЛОГІЧНІ РІШЕННЯ КОМП’ЮТИНГУ КІБЕРЗАХИСТУ

Розглядаються актуальні моделі, методи, метрики та технології комп’ютингу кіберзахисту, що застосовується у подальшому для розробка архітектури спеціалізованого процесору для паралельного моделювання та розпізнавання шкідливих загроз у потоках великих даних [2-13].

2.1 Визначення комп’ютингу кіберзахисту

Еволюція кіберпростору призводить до того, що фізичний світ втрачає свою першість, стаючи залежним від віртуального. Реальність все більше підпорядковується цифровому управлінню. Будь-яке фізичне явище знаходить своє відображення в цифровому світі, і ці цифрові копії поступово починають визначати хід реальних подій. Завдяки соціальним мережам, хмарним технологіям та периферійним обчисленням, кіберфізичний світ об'єднує людство, усуваючи необхідність у посередниках.

Кібербезпека в обчислювальній сфері (CSC) добре представлена в електронних бібліотеках IEEE Xplore та Springer. Однак, існують окремі дослідження, що стосуються активного комп'ютингу, зокрема автоматизованого виявлення та нейтралізації шкідливого програмного забезпечення без втручання людини [2, 3].

Очевидно, що об'єднання зусиль у двох перспективних галузях науки, орієнтованих на потреби ринку – безпеці та обчислювальній техніці – здатне значно покращити якість послуг, умови життя та стан навколишнього середовища. Існуючі дослідження частково стосуються активного кіберфізичного обчислення, яке передбачає використання механізмів управління для забезпечення кібербезпеки.

Передача управління безпекою від людей до кіберфізичних систем створює серйозні організаційні виклики для креативного світу. Щоб запобігти негативним наслідкам на ринку кіберфізичних і соціальних

технологій, викликаним людськими помилками, необхідно створити масштабованого "аватара безпеки" за моделлю Gartner-computing: "security assistent – digital twin – smart security robot". Цей аватар допоможе приймати більш обґрунтовані рішення.

Комп'ютинг – це галузь, яка розробляє інструменти та методи для ефективного управління реальним світом, використовуючи обчислювальні технології. Вона дозволяє контролювати та оптимізувати віртуальні, фізичні та соціальні процеси за допомогою дата-центрів, мереж, великих даних, цифрового моніторингу та інтелектуальних сервісів, що робить можливим прийняття обґрунтованих рішень на основі даних.

Комп'ютинг кіберзахисту (рис. 2.1) [9] – процес моніторингу (5) і актюації (6) метричних відношень (2) в інфраструктурі управління (3) і виконання (4) для досягнення і візуалізації (8) мети – продукції (1) при заданих ресурсах (7).

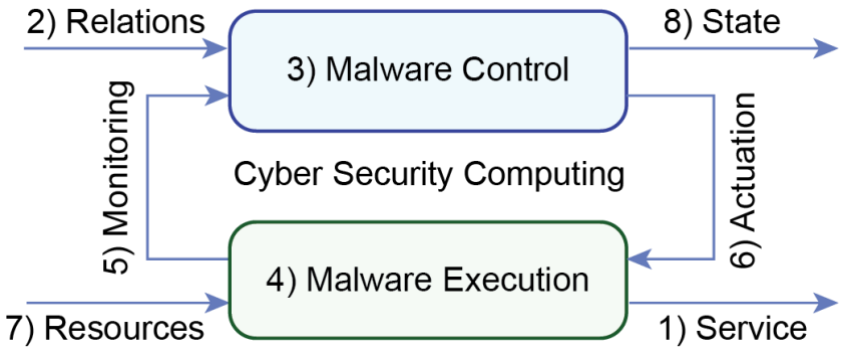

Рисунок 2.1 – Схема комп'ютингу кіберзахисту [9]

Cyber Security Computing (CSC) – це галузь, яка займається створенням систем для точного цифрового моніторингу кіберфізичного простору з метою виявлення та нейтралізації загроз. Вона включає в себе розробку інтелектуальних сервісів пошуку та аналізу, а також використання "розумних" сенсорів для відстеження деструктивних компонентів у великих даних, віртуальних, фізичних і соціальних процесах, що відбуваються в

комп'ютерних дата-центрах і мережах. Мета – забезпечити надійне та вимірюване онлайн-управління кіберзахистом.

Описаний в [9] метричний підхід до комп'ютингу, що базується на 8 взаємопов'язаних компонентах (див. рис. 2.1), пропонує теоретичну базу для формалізації та практичної реалізації будь-якого процесу в будь-якій області людської діяльності або природного світу. Завдяки цій метриці, комп'ютинг може бути застосований до широкого спектру сфер, включаючи, але не обмежуючись: космологію, біологію, ботаніку, фізику, віртуальну реальність, кібербезпеку, квантові обчислення, соціальні науки, державне управління, медицину, транспорт, інфраструктуру, науку, освіту, виробництво, спорт, відпочинок, туризм та розваги.

Процес – матеріально-енергетична взаємодія системних компонентів в часі і просторі для досягнення мети. Глобально: процес – матеріально-енергетична зміна в просторово-часовому континуумі. Локально: процес є розвиток просторового відношення компонентів (явищ) в часі [9].

Явище – компонент (системи) або фрагмент процесу в фіксований момент часу, що сприймається рецепторами, почуттями, вірою або розумом [9].

Cyber Security Computing: кібербезпека в обчисленнях – це автоматизований процес, який використовує моніторинг та управління для виявлення та реагування на загрози, що виникають внаслідок взаємодії програмного забезпечення та шкідливого коду. Він включає в себе тестування, діагностику та усунення шкідливого програмного забезпечення на основі аналізу метричних відношень.

Відношення – це система взаємопов'язаних елементів, яка задає характеристики певного процесу або явища. Важливо, що саме структура цих зв'язків визначає властивості окремих елементів, а не навпаки. Спочатку задається сигнатура відношення (тобто, правила взаємодії), а потім визначаються компоненти, які ці правила реалізують.

Наприклад, алфавіт сам по собі не має значення, поки не визначені операції (сигнатура), які дозволяють оперувати його символами. Алфавіт виступає носієм відношення, яке визначається цими операціями.

Відношення відіграють ключову роль у створенні ефективних: математичних теорій, структур даних, алгоритмів, архітектур, моделей, методів, технологій, програмно-апаратних комплексів, кіберфізичних та соціальних систем, включно з економікою, охороною здоров'я, транспортом, юриспруденцією, охороною правопорядку, кібербезпекою, екологією та державним управлінням.

Ефективність структури визначається потужністю відношення, тобто сукупністю та якістю взаємозв'язків між її компонентами. Ця потужність формує певну метрику, яка дозволяє оцінити, наскільки добре організована система.

Визначення комп'ютингу, що корисні для розуміння і практичного використання згідно до [9].

1. Комп'ютинг – це не просто обчислення, а цілеспрямований розвиток всіх складових, які беруть участь у процесі. Це означає, що ми активно працюємо над покращенням та вдосконаленням елементів, задіяних у комп'ютингу.

2. Все, що відбувається, можна розглядати як форму комп'ютингу. Це широке визначення підкреслює, що комп'ютинг – це фундаментальний процес, який лежить в основі багатьох явищ.

3. Основи комп'ютингу легко зрозуміти на простих прикладах: читання-запис, говоріння-слухання, спостереження-контроль. Ці базові дії демонструють суть обробки інформації та взаємодії.

4. Природні процеси не випадкові, а мають чітку мету та визначені правила. Це підкреслює детермінованість та цілеспрямованість процесів у природі.

5. Важливіше за окремі елементи – їхні взаємозв'язки. Елементи виникають завдяки цим зв'язкам і не можуть існувати ізольовано. Жодна частина процесу не є самодостатньою.

6. Первинним є сам процес, який створює явища та компоненти, що взаємодіють. Процес є джерелом, з якого виникають окремі елементи та їхня взаємодія.

7. Дилема "курка чи яйце" вирішується: обидва є результатом еволюційного процесу або комп'ютингу. Це підкреслює, що складні явища виникають внаслідок поступового розвитку.

8. Еволюція за Дарвіном – це приклад комп'ютингу в природі, де види розвиваються в часі та просторі. Еволюція є процесом обробки інформації та адаптації до навколишнього середовища.

9. Соціальний комп'ютинг – це розвиток відносин між владою та громадянами для досягнення спільних цілей. Це процес обробки інформації та прийняття рішень у суспільстві.

2.2 Метрика комп’ютингу кіберзахисту

Елементарна основа виміру є відношення між двома компонентами: процесами або явищами. Ця взаємодія зазвичай характеризується асиметрією між компонентами, а мірою цієї асиметрії є їхня відповідність або невідповідність (виражена як "так/ні" або "істина/хибність"), що і визначає метрику. Як правило, в процесі – це відношення нерівності пари компонентів, яке вимірюється ставленням рівності (xor, not-xor), що становить сутність метрики.

Кожен компонент існує лише у взаємозв'язку з іншими, оскільки будь-яка операція, що його визначає, по суті є відношенням між компонентами. Це справедливо навіть у випадку рефлексивного відношення, коли компонент пов'язаний сам із собою. Таким чином, елемент не може бути розглянутий ізольовано, а лише як частина певної системи відношень.

Взаємодія протилежних і нерівнозначних явищ з плином часу призводить до формування стабільних систем або еволюційних процесів. Навпаки, взаємодія схожих явищ веде до нестабільності та деградації. Зміна, що виникає внаслідок взаємодії протилежностей, є результатом їх об'єднання. Це правило поширюється на всі розглянуті пари відносин. Симетрія та рівність між компонентами системи унеможливлюють її розвиток. Рівність компонентів сигналізує про зупинку еволюції, що підтверджується відсутністю змін у їхній взаємодії. В процесі еволюції компоненти системи трансформуються один в одного. Відносини між компонентами породжують нові елементи, але не навпаки. Головна мета еволюції – перехід від одного явища до іншого.

CSC – це процес, що включає в себе тестування, моніторинг та діагностику, спрямовані на виявлення та нейтралізацію шкідливих компонентів (malware) в кіберфізичному середовищі. Він базується на аналізі метричних співвідношень між шкідливим та легітимним програмним забезпеченням (software) для ініціювання дій з усунення загроз.

CSC-процес передбачає відстеження взаємодії між malware та software в часі та просторі, використовуючи моніторинг та активацію на основі метричних даних, з метою ефективного видалення malware з урахуванням доступних ресурсів.

Malware-функціональність (MF) – це сукупність взаємопов'язаних частин коду, які разом реалізують шкідливу дію програми в цифровому середовищі, впливаючи на різні аспекти програмного забезпечення.

Malware-змінна (MV) – це набір можливих значень, які описують поведінку шкідливого об'єкта. Ці значення, взяті разом, показують, як об'єкт реалізує свою шкідливу функціональність.

Логічний malware-елемент (ML) – це спосіб перетворення складного значення змінної у простіший двійковий код (послідовність бітів), що дозволяє комп'ютеру обробляти цю інформацію.

Значення (LV) змінної – це окрема, унікальна характеристика об'єкта, яка відрізняється від інших характеристик, але разом з ними утворює повний набір можливих значень.

2.3 Архітектура комп’ютингу кіберзахисту

Таким чином, проглядається структурована ієрархія введених понять, рис. 2.2:

$$<CSC – MF – MV – ML – LV>, \quad (2.1)$$

яка формує можливі архітектурні рішення malware-комп'ютингу.

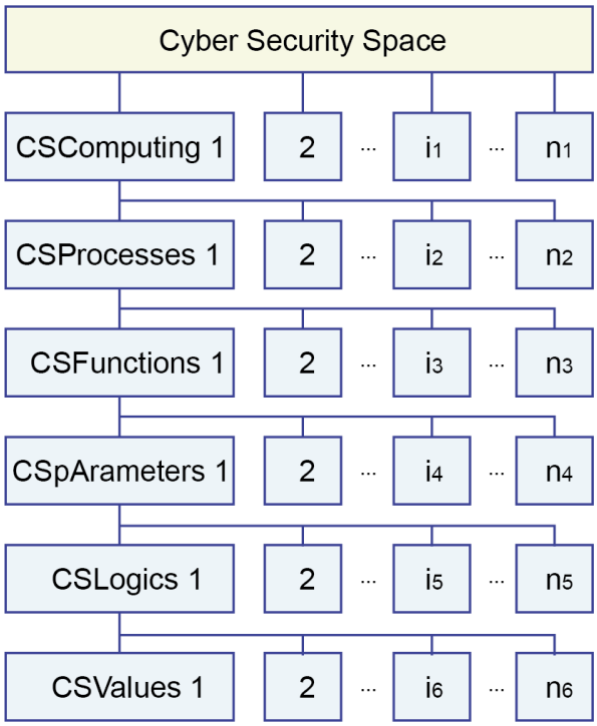

Рисунок 2.2 – Схема ієрархії комп'ютингу кіберзахисту [14]

На ML-рівні архітектури будується логічна схема, де кожен елемент представлений багатозначною змінною. Ця змінна, по суті, є кубітним вектором, який може мати більше одного "1". Ця особливість кубітів

дозволяє ефективно представляти та паралельно обробляти складні функції шкідливого ПЗ.

Для квантового моделювання на основі цих кубітних структур даних, вхідні дані (символи) кодуються за допомогою спеціальних таблиць, які однозначно пов'язують кожну змінну з її унітарним представленням.

Кожна змінна відповідає ключовому слову (терміну), яке часто зустрічається у вхідних даних. Набір цих ключових слів утворює унікальний набір змінних, що описують процес шкідливого ПЗ. Значення кожної змінної представлені синонімами відповідного ключового слова, формуючи клас еквівалентності, який визначає багатозначність змінної.

Всі ці змінні разом утворюють простір, що описує процес шкідливого ПЗ. У цьому просторі визначаються типові, практично важливі функції шкідливого ПЗ, які моделюються у вигляді логічних кубітних схем. Ці схеми використовуються для моделювання вхідних потоків даних, отриманих з різних джерел, таких як хмара, мережа, комп'ютери або мобільні пристрої.

2.4 Моделі комп’ютингу кіберзахисту

Спеціалізовані архітектури та традиційні структури використовуються в кіберфізичних системах. Відокремлюються метричний моніторинг і цифрове керування. Мета – автоматизоване прийняття рішень, виявлення та ідентифікація шкідливого програмного забезпечення, а також визначення ступеня відповідності вхідних даних заданому деструктивному шаблону. Оцінка відповідності базується на метриці відстаней. Моделі розробляються з урахуванням їхньої апаратної реалізації для онлайн-моделювання. Це дозволить генерувати автоматичні керуючі сигнали, які не потребують участі людини та ефективно нейтралізують шкідливий код.

Логічні кубітні структури здатні ідентифікувати шкідливий код, що надходить на спеціалізований комп'ютер, і видаляти його з програм.

Кожен параметр шкідливого ПЗ може мати позитивні та негативні значення (можливі й множинні варіанти). Однак, можна обмежитися лише позитивними зразками, що базуються на конструктивних параметрах або атрибутах. Такі архітектури, які можна розглядати як логічні процесори, формують еталонні характеристики шкідливих процесів і явищ.

Квантові обчислення, завдяки своїй здатності до паралельної обробки даних, успішно застосовуються для розв'язання складних комбінаторних задач, імітуючи обчислення, що виконуються на звичайних комп'ютерах [4-6]. Для опису логічних елементів ефективно використовуються таблиці істинності або кубічні покриття, які є зручними структурами даних для задач CSC-комп'ютингу та пошуку потрібної інформації [7, 8]. Автоматичне створення кубітних покриттів для реалізації різних функцій є ключовим, але складним завданням, без якого неможливий аналіз великих обсягів даних [9-13]. Нижче наведено аналітична модель W кубітно-логічного процесора CSC-комп'ютингу. Вона оперує двома матрицями: матрицею універсумів U примітивів та матрицею кубітних функціональностей Q, а також логічними примітивами L, які об'єднують функціональності в комбінаційну схему CSC-процесора:

$$
\begin{aligned}
&W = (U, Q, L),\\
&U = (U_1, U_2, ..., U_i, ..., U_n);\\
&\bigcup_{i-1}^{n} U_i = U;\ U_i \bigcap_{i,k=1,n}^{i\neq k} U_k = \varnothing;\\
&Q = (Q_1, Q_2, ..., Q_i, ..., Q_n);\\
&\bigcup_{i-1}^{n} Q_i = Q;\ Q_i \bigcap_{i,k=1,n}^{i\neq k} Q_k = \varnothing;\\
&Q_i = (Q_{i1}, Q_{i2}, ..., Q_{ij}, ..., Q_{im});\ Q = [Q_{ij}];\\
&U_i = (U_{i1}, U_{i2}, ..., U_{ij}, ..., U_{im});\ U = [U_{ij}];\\
&L = f[Q] = (Q_1 \circ Q_2 \circ, ..., \circ Q_i \circ, ..., \circ Q_n)\\
&\circ = \{\wedge, \vee, \oplus\};\\
&U_{ij} \in U_i \in U;\ Q_{ij} \in Q_i \in Q;\ Q_i \in U_i;\ Q \in U;\\
&Q_{ij} = 1 \leftarrow \max \mu(R, U_{ij}).
\end{aligned}
\qquad (2.2)
$$

Для виявлення шкідливого коду, вхідний потік даних R=X порівнюється з еталонним зразком U (метрика-універсум). Аналізатор-компаратор визначає, наскільки R відрізняється від U, обчислюючи функцію приналежності. Найбільше значення цієї функції вказує на найбільш ймовірну аномалію і кодується в стані кубіта: $Q_{ij} = 1 \square \max \mu(R, U_{ij})$.

Архітектура метричної взаємодії U-матриці універсумів з потоком даних R для обчислення функцій належності μ(R, U), з метою отримання Q-матриці значень і подальшого L-об'єднання кубітів в комбінаційну схему кіберсоціального процесора, представлена на рис. 2.3 [9].

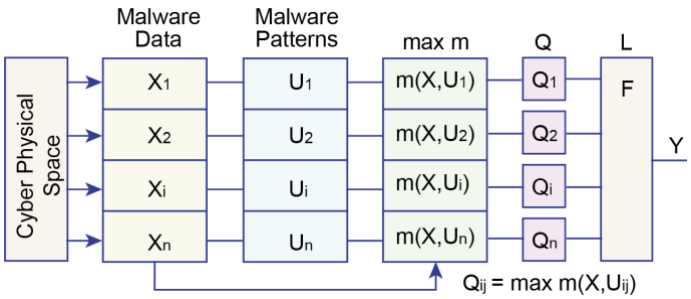

Рисунок 2.3 – Архітектура для синтезу CSC-процесора [9]

Вхідні дані R, що імітують масштабні руйнівні процеси, мають структуру, аналогічну U- та Q-матрицям, а також логічній схемі процесора. Алгоритм побудови Q-матриці базується на знаходженні найбільшого значення функції належності для кожного вхідного кадру змінної до одного зі значень відповідного рядка матриці універсумів (U-матриці). Порівнюючи таким чином всі координати U-матриці, формуються окремі координати кубітної матриці. Кожен рядок цієї матриці представляє базову функціональність для відповідної змінної. Об'єднавши всі рядки Q-матриці, отримуємо логічну схему комбінаційного процесора (CSC-процесора), здатного моделювати будь-який вхідний вплив. Це дозволяє визначити, наскільки цей вплив відповідає заданому еталону деструктивного процесу або явища.

Для аналізу шкідливих потоків даних використовується метод, що базується на створенні кубітів за допомогою логічних CSC-еталонів. Вхідні фрагменти даних обробляються одним або декількома логічними елементами, які визначають метрику CSC-процесу.

Моделювання потоку шкідливих даних призводить до формування бінарних значень, що відображають ступінь відповідності еталону в кубітному векторі кожного логічного елемента, який відповідає певному параметру. Це досягається шляхом вимірювання функції приналежності вербальних даних до кожного значення заздалегідь визначеного набору примітивів логічної змінної. Таким чином, автоматично генеруються кубітні представлення CSC-функціональності.

Для повноцінного опису CSC-процесу (або явища) необхідно визначити повний набір параметрів (змінних). Це робиться за допомогою аналізу великих даних, який виявляє ключові поняття (слова), що максимально відрізняються одне від одного. Ці поняття представляють класи еквівалентності, які охоплюють всі CSC-змінні.

Примітиви та класи еквівалентності – базові елементи (примітиви) розглядаються як окремі класи еквівалентності, що визначають всі можливі значення певної змінної. Набір цих класів еквівалентності формує універсум змінних вищого рівня.

Аналітичний синтез – ці властивості використовуються для створення повного набору змінних, які описують цифровий образ CSC-процесу, формуючи його "еталонну функціональність".

Наприклад, створення віртуального асистента/цифрового двійника/розумного робота: для створення віртуального асистента, цифрового двійника або розумного робота, який реагує на зовнішні дані, потрібно виконати наступні кроки:

1) створення універсуму змінних-примітивів – визначити всі базові змінні, необхідні для опису функціональності CSC-процесу;

2) створення U-матриці – створити матрицю, що містить всі можливі значення кожної змінної-примітиву в рамках CSC-процесу;

3) створення Q-матриці – створити матрицю, що містить конкретні значення-примітиви для кожної змінної, представлені у вигляді кубіт-векторів;

4) перевірка повноти та примітивізму – перевірити U-матрицю на повноту (чи охоплює вона всі необхідні змінні та значення) та примітивізм (чи є змінні та значення достатньо базовими).

Таким чином, щоб створити цифрове представлення CSC-процесу, потрібно визначити всі ключові параметри (змінні) та їх можливі значення. Це робиться за допомогою аналізу даних, який виявляє базові поняття та їх взаємозв'язки. Отримані дані використовуються для створення матриць, які описують всі можливі стани процесу. Потім ці матриці перевіряються на повноту та точність.

Отримані після синтезу кубітних векторів результати з Q-матриці, що представляють собою стани кубітів, передаються на інтегратор L. Цей інтегратор, використовуючи логічну функцію "I" (або іншу, наприклад, "HI-I"), об'єднує ці стани в єдиний бінарний вихід: 1 або 0. Цей вихід інтерпретується як результат моделювання, що вказує на відповідність досліджуваного процесу (наприклад, CSC-процесу) характеристикам шкідливого програмного забезпечення.

Отже, logic-процесор, побудований на основі квантових структур даних (Q-матриць), здатний в режимі реального часу моделювати складні CSC-процеси та явища, які неможливо ефективно відтворити на класичних комп'ютерах. Це стає можливим завдяки здатності квантових обчислень обробляти складні та нечіткі дані, що особливо важливо при аналізі поведінки шкідливого ПЗ, формалізація якого для традиційних цифрових моделей є надзвичайно складною задачею.

Для створення еталонної моделі CSC-процесу або явища спочатку визначають ключові параметри, що його характеризують. Для кожного з цих

параметрів створюється набір значень, які потім кодуються у вигляді кубітного вектора, що представляє логічний елемент. Ці логічні елементи, що відповідають ключовим параметрам, поєднуються за допомогою логічних операцій (І, АБО, НІ, XOR) для моделювання взаємозв'язків між параметрами. Результатом є визначення, чи відповідає вхідний процес або явище заданим стандартам.

CSC-комп'ютинг можна розглядати як кіберфізичну систему, яка використовує інтелектуальне хмарне управління для моніторингу та контролю CSC-процесів. Це досягається за допомогою точного цифрового моніторингу, що охоплює: інтелектуальну електронну інфраструктуру, персонал компанії з комп'ютерами та гаджетами, а також транзакції та процеси, що відбуваються в певний час і місці. Система CSC-комп'ютингу складається з трьох основних взаємопов'язаних компонентів: хмарного інтелектуального управління, електронної CSC-архітектури та кіберфізичного простору (рис. 2.4).

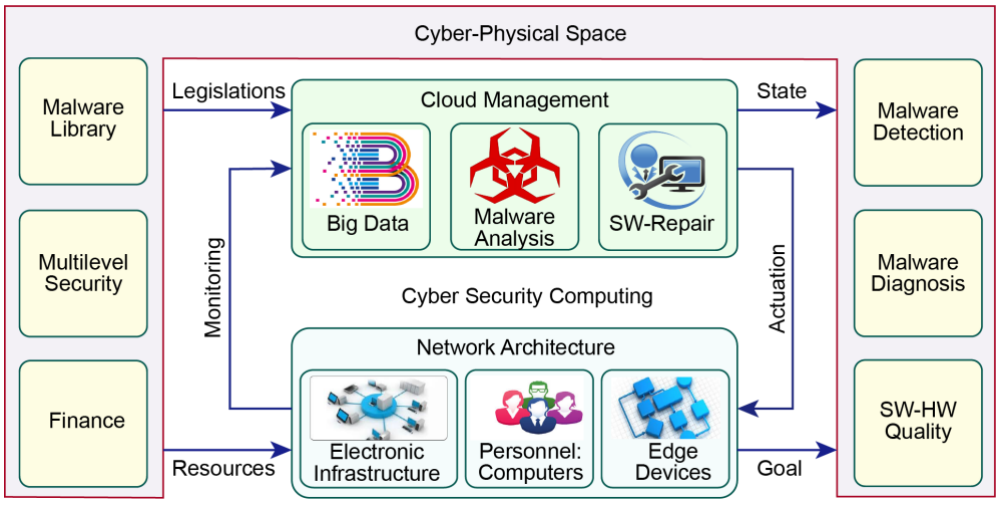

Рисунок 2.4 – CSC-комп'ютинг моніторингу та управління процесами [9]

Хмарні сервіси для моніторингу та нейтралізації шкідливого програмного забезпечення працюють за принципом: виявлення – аналіз – реагування. Вони збирають великі обсяги даних з різноманітних датчиків та

комп'ютерних систем, а потім використовують інтелектуальний аналіз даних, зокрема, глибоке навчання (CNN, DNN) та машинне навчання (ML), для виявлення та оцінки загроз. На основі цього аналізу система формує та застосовує цифрові команди для управління інфраструктурою з метою видалення шкідливого ПЗ та забезпечення високої якості кібербезпеки.

Ця система хмарних обчислень (CSC-комп'ютинг) безпосередньо взаємодіє з кіберпростором (інтернетом), який є необхідним каналом для вхідних та вихідних даних. Крім того, на систему впливають законодавчі норми, що регулюють діяльність компанії, та доступні ресурси (фінанси, матеріали), необхідні для захисту процесів створення продуктів та послуг. Важливим показником ефективності системи є її поточний стан, який відображає рівень розвитку та захищеності комп'ютерної інфраструктури.

CSC-комп'ютинг – це технологія ефективного хмарного управління, спрямована на значне скорочення непродуктивних витрат та збільшення прибутковості. Вона базується на оперативному онлайн-моніторингу процесів з використанням сучасних кібертехнологій, таких як Інтернет речей (IoT), кіберфізичні системи, хмарні обчислення, електронна інфраструктура, аналіз великих даних, штучний інтелект, блокчейн-смарт-контракти, електронний документообіг та інтернет.

Принципи реалізації:

1) відстеження роботи програмного забезпечення за допомогою спеціального агента, незалежно від фізичного розташування пристрою (віддалений моніторинг без прив'язки до географії);

2) комплексний моніторинг усіх пристроїв для інтелектуального аналізу даних, що дозволяє автоматично керувати компонентами системи та оперативно змінювати процеси в режимі реального часу (автоматизації управління на основі аналізу даних);

3) автоматизований моніторинг з можливістю онлайн-управління, що мінімізує необхідність втручання людини. Це ключове, але ще не вирішене

завдання для ринку систем управління ланцюгами поставок (CSC) (повна автоматизація та виклики перед CSC-ринком).

Відстеження шкідливого програмного забезпечення, яке самостійно генерується кіберфізичними системами без участі людини, і при цьому не передбачає активного втручання для нейтралізації його наслідків, не є комерційно привабливим у сучасній кіберкультурі. Вихід із ситуації очевидний: потрібна система моніторингу, яка здатна в режимі реального часу керувати процесами, використовуючи інтелектуальні алгоритми або смарт-контракти для забезпечення законної взаємодії в кіберпросторі. Програмний код повинен автоматично реагувати на події, аналізувати їх та вживати заходів, імітуючи соціальну взаємодію <факт – оцінка – дія>. Фактично, це зводиться до створення алгоритму, який обробляє вхідні дані та генерує керуючі сигнали для компонентів кіберфізичної інфраструктури, що працює в рамках парадигми Інтернету речей (IoT).

CSC-система складається з наступних ключових елементів [12]:

1) внутрішнє середовище компанії – це сукупність правил, норм і цінностей, що регулюють діяльність організації. Вони базуються на законодавстві, статуті, внутрішніх документах, а також на історичному досвіді, традиціях і корпоративній культурі;

2) стратегічне бачення – чітко сформульована мета або напрямок розвитку, який є зрозумілим для ринку та надихає співробітників на досягнення високих результатів;

3) цифрове управління – ефективна система управління, що використовує хмарні технології для автоматизації процесів, мінімізації людського фактору в моніторингу та прийнятті рішень, що є критично важливим для успіху на ринку;

4) інфраструктура – створені умови для продуктивної роботи, які включають комфортне робоче місце, якісне харчування та можливості для відпочинку, доступні як в офісі, так і віддалено, цілодобово;

5) людський капітал – кваліфіковані співробітники, які створюють продукти та послуги, що пропонуються на ринку. Їхні знання та навички є найціннішим активом компанії, а їхня цінність визначається унікальним набором компетенцій.

2.5 Матрична структура даних для кодування шкідливих загроз

Суть проблеми CSC-комп'ютингу полягає у важкості чіткого та однозначного опису логіки шкідливого програмного забезпечення (malware). Необхідно перетворити цю логіку на передбачувані та детерміновані функції, усуваючи будь-яку випадковість чи невизначеність. Замість використання евристичних методів, актуальним завданням для ринку є автоматизація процесів синтезу та аналізу логічних схем CSC-обробки, що дозволить моделювати та прогнозувати конфлікти, пов'язані з malware. Для вирішення цієї проблеми пропонується перетворити великі обсяги даних у структуровану матричну двійкову форму. Ця форма унітарно кодує всі можливі значення змінних, що характеризують malware, утворюючи повний набір базових елементів. Запропонований метод вирішення базується на синтезі класів еквівалентних відношень на множині змінних P:

$$P = \{P_1, P_2, \dots, P_i, \dots, P_j, \dots, P_n\}, P_i \cap P_j = \emptyset, \quad (2.3)$$

де кожна з них $P_i = \{P_{i1}, P_{i2}, \dots, P_{ik}, \dots, P_{ir}, \dots, P_{in}\}$ приймає універсальну множину malware-значень, що створюють між собою еквівалентні відношення $P_{ik} \sim P_{ir}$ і утворюють при цьому порожні перетини $P_{ik} \cap P_{ir} = \emptyset$.

1. У контексті CSC-комп'ютингу, метрика визначає спосіб обчислення відстаней d_i між різними процесами та явищами, які існують у просторі, визначеному набором параметрів. Цей метод вимірювання відстаней повинен відповідати певним правилам, зокрема аксіомі циклічного конволюційного

замикання:

$$D = \sum_{i=1}^{n} d_i = 0 \tag{2.4}$$

2. Вимірювання розглядається як процедура визначення відстані між кінцевою множиною процесів або явищ, відмінних від нуля.

3. Параметри – це логічні змінні $P = \{P_1, P_2, \dots, P_i, \dots, P_n\}$ для опису процесу або явища.

4. Змінні визначаються за їх значеннями

$$P_i = \{P_{i1}, P_{i2}, \dots, P_{ij}, \dots, P_{in}\}, \tag{2.5}$$

яких може бути мінімум два.

5. Матриця універсумів, позначена як $U = [P_{ij}] = [U_{ij}]$, являє собою впорядкований набір змінних та відповідних їм значень, що використовується для кількісної оцінки процесу або явища. Унітарно кодована матриця U характеризується наявністю одиничних значень у кожній її позиції. Матрицю універсумів U можна трансформувати в єдиний вектор шляхом послідовного об'єднання її рядків $P = (P_1 * P_2 * \dots * P_i * \dots * P_n)$.

6. Матриця шкідливого програмного забезпечення (Q), що позначається як $Q = [Q_{ij}]$, являє собою набір конкретних значень змінних, взятих з універсальної матриці $Q \in U$,, яка охоплює всі можливі значення. Цей набір значень формує унікальний "відбиток" певного процесу або явища, пов'язаного зі шкідливим ПЗ. Для зручності представлення, ці значення змінних часто кодуються у вигляді двійкової матриці, де кожен елемент є 0 або 1.

7. Матриця вхідних даних $X = [X_{ij}]$, що містить двійкові значення, є підмножиною універсальної матриці $X \in U$. Вона представляє собою фрагмент даних, що описує конкретний реальний процес або явище.

8. Матриця вимірювань $Y = [Y_{ij}]$, що є підмножиною двійкових значень U ($Y \in U$), формується шляхом поелементної XOR-операції ($\oplus$) між матрицями $Q = [Q_{ij}]$ та $X = [X_{ij}]$. Таким чином, $Y = [Y_{ij}] = [Q_{ij}] \oplus [X_{ij}]$. Ця операція виявляє відмінності між відповідними координатами матриць Q та X, де Q представляє malware, а X – фрагмент обчислювального процесу або явища.

9. Відстань – це числова міра, яка показує, наскільки відрізняються між собою два процеси або явища. Вона обчислюється в певних одиницях, виходячи з координат, які описують ці процеси/явища. Відстань визначається шляхом підрахунку одиничних координат у матриці вимірювань: $d(Q, X) = \sum_{j=1,m}^{i=1,n} Y_{ij}$.

10. Функція відмінності вимірює ступінь несхожості між двома об'єктами, представленими у вигляді матриць. Вона обчислюється як кількість координат, в яких об'єкти відрізняються, поділена на загальну кількість координат:

$$\mu = \frac{d(Q,X)}{n \times m} = \frac{\sum_{j=1,m}^{i=1,n} Y_{ij}}{n \times m}. \quad (2.6)$$

2.6 Висновки до розділу 2

Виконано аналіз моделей, методів, метрик, структур даних та технологічних рішень комп’ютингу кіберзахисту для подальшої розробки архітектури спеціалізованого процесору для паралельного моделювання та розпізнавання шкідливих загроз у потоках великих даних.

3 АРХІТЕКТУРА СПЕЦІАЛІЗОВАНОГО ПРОЦЕСОРУ ДЛЯ МОДЕЛЮВАННЯ ШКІДЛИВИХ ЗАГРОЗ

Розробляється архітектура спеціалізованого процесору для моделювання шкідливих загроз. Наведено алгоритм роботи процесору.

3.1 Процесорна архітектура комп’ютингу кіберзахисту

Описується процесорна архітектура для активного онлайн кіберзахисту, призначена для кіберфізичних систем. Ця архітектура працює шляхом відстеження вхідних даних, які можуть містити шкідливе програмне забезпечення (malware). Потім ці дані моделюються на основі відомих шаблонів шкідливих функцій. Це дозволяє в режимі реального часу виявляти та видаляти шкідливі компоненти.

Логічна структура, зображена на рис. 3.1, представляє собою обчислювальну архітектуру для аналізу шкідливого програмного забезпечення.

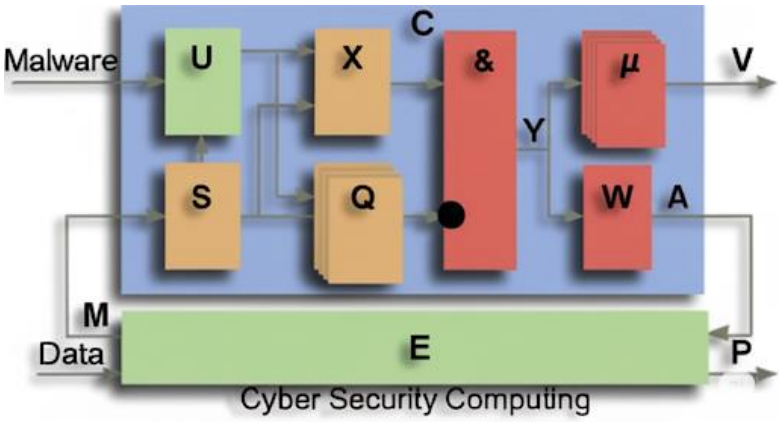

Рисунок 3.1 – Архітектура паралельного CSC-комп'ютингу, що використовує матричні обчислення та логічні операції

Вона включає в себе всі вісім основних компонентів універсального обчислювача, які взаємодіють між собою для забезпечення функціональності аналізу:

1) ініціалізація команди на вході R для виконання CSC-процесу, який починається з отримання інформаційних D-ресурсів, що надходять на виконавчий механізм E;

2) виконавчий механізм E ініціює збір даних за допомогою сенсорів, які передають інформацію через шину M, формуючи потік даних S;

3) потік даних S використовується для створення U-матриці, яка представляє собою універсум змінних, що описують CSC-процес. Ця U-матриця є базою для формування X-матриці. X-матриця містить вектори вхідних даних для кожної змінної і використовується в ітеративному моделюванні відносно Q-матриці;

4) Q-матриця представляє собою набір двійкових векторів, кожен з яких описує типовий зразок шкідливого програмного забезпечення (malware) у кубітному просторі. Ці вектори охоплюють всі можливі змінні, що характеризують malware. Використовуючи операцію "I" (AND) над цими векторами, можна визначити ступінь відповідності досліджуваного об'єкта до еталонного malware-патерна, тобто обчислити функцію приналежності μ. Інакше: Q-матриця – це спосіб кодування характеристик відомих зразків шкідливого коду у вигляді двійкових векторів, що дозволяє, за допомогою логічної операції "I", оцінити, наскільки певний об'єкт схожий на відомий malware.

5) функція приналежності μ з виходом візуалізації стану V CSC-процесу, а також відповідний Y як числове значення кількості різних двійкових однойменних координат;

6) матриця Y обчислюється шляхом паралельного застосування операції порівняння до матриць X і Q:

$$X \wedge notQ = Y, \tag{3.1}$$

яка перетворює дані з U-матриці (представленої матрицею Y) у вербальні команди W для виконавчих пристроїв. Ці команди передаються по шині A і запускають відповідні обчислення;

7) обчислювальні процедури спрямовані на усунення розходжень між матрицями X та Q, яка є еталонною для malware-патерну, шляхом корекції координат X-матриці за допомогою інфраструктури E, що забезпечує виконання CSC-процесу компанії для отримання результату на виході P.

Архітектура CSC-комп'ютингу використовує паралельну обробку для швидкого виявлення шкідливого програмного забезпечення. Вхідні дані (X-матриці) обробляються паралельно за допомогою Q-матриць, що дозволяє створити μ-матриці, які відображають ступінь схожості вхідних даних з відомими зразками шкідливого коду. Мінімальна відмінність та скалярні оцінки використовуються для точної ідентифікації та нейтралізації загроз.

Опис та ключові особливості моделі кубітно-матричного процесора, що відповідає архітектурі (див. рис. 3.1):

1. Обробка даних на основі кубітних матриць використовує кубітні матриці для обчислень, характерних для CSC-комп'ютингу. Архітектура включає блоки управління C та виконання E, які взаємодіють через шини моніторингу M та актюації A.

2. Інтерфейси блоків управління та виконання – блок управління отримує команди через вхід R і надає інформацію про стан CSC-процесу через вихід V. Блок виконання отримує вхідні дані через вхід D і надає результати обчислень або сервіси через вихід P. Всі вісім компонентів визначають функціональність CSC-комп'ютингу.

3. Початок обчислень з вхідного потоку даних – CSC-комп'ютинг починається з аналізу вхідного потоку даних (S), отриманого від сенсорів, які контролюють CSC-процес.

4. Створення матриць для моделювання – процес передбачає створення U-матриці, яка представляє універсум змінних, кожна з яких описується

вербальними значеннями. Ця U-матриця служить основою для створення X-матриці вхідних даних, яка потім використовується для моделювання разом з попередньо визначеними Q-матрицями.

5. Виявлення шкідливого ПЗ на основі Q-матриць – Q-матриці представляють собою набір відомих шаблонів шкідливого програмного забезпечення (malware). За допомогою операції "I"(&), процесор може паралельно обчислювати n матриць, що дозволяє швидко виявляти відповідності з цими шаблонами:

$$Yi = (X \wedge notQi),\ i=1,\ldots,n, \tag{3.2}$$

моделювання, проаналізувавши які на мінімальну кількість одиничних координат min(Yi=1), i=1,…,n, модна виявити номер і матриці, що має мінімальне значення з n функцій приналежностей

$$\mu = \min_i \mu_i \leftarrow \mu_i = \sum_{j=1,k}^{r=1,m} Y_{ijr}, \tag{3.3}$$

6. Функції приналежності кількісно визначають розбіжності між відповідними бінарними координатами матриці X та кожної з n матриць Q. (кількісна оцінця розбіжностей).

7. Це дає можливість створити матрицю W, що містить вербальні сигнали для керування, які відповідають одиничним значенням у вихідній матриці Y (зв'язок між вихідною матрицею та керуючими сигналами).

8. Вихідна матриця Y містить вербальні значення U-матриці з мінімальним значенням функції приналежності (min μ). Вони запускають обчислення у виконавчому механізмі E, щоб мінімізувати розбіжності між матрицею X та матрицею Q, що представляє шкідливий патерн з min μ. Це досягається шляхом корекції координат матриці X, що забезпечує оптимальне досягнення мети P процесу CSC.

3.2 Алгоритм

Алгоритм (рис. 3.2) керує обчислювальними операціями процесора, визначаючи, як і коли він аналізує дані для виявлення шкідливих програм. Мета – розпізнати шкідливі патерни у вхідних даних і, якщо вони знайдені, згенерувати сигнали для їх нейтралізації або знищення.

Рисунок 3.2 – Алгоритм CSC-комп'ютингу

Процес починається з:

1. Ініціалізації – запуск алгоритму.

2. Смисловий аналіз – аналіз вхідних даних (S), які надходять від входу D та сенсорів M цифрової інфраструктури.

3. Перевірка U-матриці – перевірка, чи існує вже готова U-матриця. Якщо так, перехід до кроку 6. Якщо ні, то:

4. Розбиття на класи еквівалентності та вилучення універсуму malware – текстові фрагменти даних розбиваються на групи (класи еквівалентності). З цих груп вилучаються основні елементи, що характеризують шкідливе

програмне забезпечення (змінні-примітиви). Для кожного з цих елементів визначається набір можливих значень, що разом утворюють U-матрицю. Ця матриця служить шаблоном для подальшого аналізу.

5. Синтез кубітних Q-матриць – на основі U-матриці створюються кубітні Q-матриці, які представляють собою шаблони шкідливих програм.

6. Використовується кубітна X-матриця, яка слугує вхідними даними для подальших обчислень.

7. Над цією матрицею паралельно виконується операція "I" з інвертованими кубітними матрицями Qi, що призводить до створення n матриць Yi, де кожна Yi є результатом операції Yi=(X∧notQi). Далі, для кожної з цих матриць Yi обчислюється кількість одиничних координат min(Yi = 1).

8. Порівняння кількості одиничних координат у кожній з n матриць Yi дозволяє ідентифікувати номер і тієї матриці, яка має найменше значення, що відповідає мінімуму з n функцій приналежності

$$\mu = \min_i \mu_i \leftarrow \mu_i = \sum_{j=1,k}^{r=1,m} Y_{ijr}, \qquad (3.4)$$

отримані різниці між відповідними бінарними координатами матриці X та кожної з n матриць Q перетворюються на числові значення. Це дозволяє:

9. Створити матрицю W, що містить вербальні сигнали для керування, яка відповідає одиничним значенням координат вихідної матриці Y з мінімальним значенням μ. Ці сигнали представлені у вигляді вербальних значень U-матриці.

10. Якщо μ не дорівнює нулю, то:

11. Запускаються обчислювальні процеси у виконавчому механізмі E. Ці процеси спрямовані на мінімізацію розбіжностей між матрицею X та матрицею Q, що представляє зразок шкідливого ПЗ з мінімальним μ. Розбіжності усуваються шляхом коригування координат матриці X, що

забезпечує оптимальне досягнення мети P CSC-процесу. Якщо ж μ не дорівнює нулю, алгоритм завершує роботу з поточною матрицею вхідних даних. Це забезпечує реалізацію CSC-комп'ютингу, націленого на знищення шкідливого ПЗ шляхом цифровізації, автоматизації та оптимізації CSC-процесу в просторі та часі при створенні сервісу або продукту.

3.3 Висновки до розділу 3

Використання матричної структури даних дозволяє значно прискорити паралельну обробку даних про шкідливе програмне забезпечення (malware). Це дає можливість швидше виявляти типові ознаки (патерни) malware у вхідних потоках даних. На основі виявлених патернів генеруються сигнали для усунення malware або виявлення відхилень від еталонних зразків.

ВИСНОВКИ

1. Проаналізовано технологічні тенденції у сфері кібербезпеки, що визначені компанією Gartner на 2025 рік. Вони зумовлені поєднанням захисту програмного забезпечення для мобільних пристроїв з апаратними рішеннями безпеки для підвищення надійності зберігання конфіденційних даних. Апаратні рішення, як розробка спецпроцесорів кіберзахисту, є актуальними та становлять предмет для дослідження, розвитку та впровадження комп’ютерними інженерами.

2. Проаналізовано актуальні моделі, методи, метрики та технології комп’ютингу кіберзахисту, що застосовується у подальшому для розробка архітектури спеціалізованого процесору для паралельного моделювання та розпізнавання шкідливих загроз у потоках великих даних.

3. Розроблено архітектуру логічного процесора, що використовує інтерпретативні кубітні матричні моделі та методи CSC-комп'ютингу для паралельного моделювання та розпізнавання malware-патернів у потоках великих даних. Ця архітектура дозволяє автоматично синтезувати та аналізувати логічні схеми, орієнтовані на моніторинг і управління CSC-процесами та явищами, з метою виявлення та усунення деструктивних компонентів у кіберпросторі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Gartner Identifies the Top Cybersecurity Trends for 2025. – Sydney, Australia. – March 3, 2025. [https://www.gartner.com/en/newsroom/press-releases/2025-03-03-gartner-identifiesthe-top-cybersecurity-trends-for-2025]

2. Lehto, Martti, Neittaanmäki, Pekka Cyber Security: Analytics, Technology and Automation, Springer, 2015. 269 p.]

3. Orojloo Hamed, Mohammad Abdollahi Azgomi. Modelling and evaluation of the security of cyber-physical systems using stochastic Petri nets. IET Cyber-Physical Systems: Theory & Applications (2019), 4 (1), P. 50-57.]

4. Benenti G. Principles of Quantum Computation and Information / G. Benenti, G. Casati, G. Strini. – Volume 1: Basic Concepts. – Singapore: World Scientific. – 2004.- 272 p. https://doi.org/10.1142/5528

5. Hiroshi I. Quantum Computation and Information. From Theory to Experiment / I. Hiroshi, H. Masahito. – Berline, Germany. – Springer, 2006. – 234 p. [https://www.researchgate.net/profile/Masahito-Hayashi/publication/225991383_Entanglement_and_Quantum_Error_Correction/links/0fcfd50e623952377b000000/Entanglement-and-Quantum-Error-Correction.pdf]

6. Nielsen M.A. Quantum Computation and Quantum Information / M.A. Nielsen, I.L. Chuang. – Cambridge University Press. – 2010. – 710 p. [https://www.academia.edu/41154803/Quantum_Computation_and_Quantum_Information_by_Nielsen_and_Chuang].

7. Abramovici M. Digital System Testing and Testable Design / M. Abramovici, M.A. Breuer, A.D. Friedman. – Comp. Sc. Press. – 1998. – 652 p. [https://www.academia.edu/4746659/Digital_systems_testing_and_testable_design].

8. Vector-Qubit models for SoC Logic-Structure Testing and Fault Simulation / [V. Hahanov, W. Gharibi, S. Chumachenko et al.] // 16th International Conference on the Experience of Designing and Application of CAD Systems (CADSM). Lviv,

Ukraine, 2021: proceedings. – IEEE, 2021. – P. 24–28. https://doi.org/10.1109/cadsm52681.2021.9385266

9. Hahanov V. Cyber Physical Computing for IoT-driven Services / V. Hahanov. – New York: Springer, 2018. – 279p. 10.1007/978-3-319-54825-8

10. Quantum memory-driven method for test synthesis based on qubit data structures / [V.I. Hahanov, I.B. Iemelianov, M.M. Liubarskyi, S.V. Chumachenko, E.I. Litvinova] // Electronic Modeling. – 2018. – Vol. 40, №1. – P. 63-80. https://doi.org/10.15407/emodel.40.01.063

11. Qubit Data Structures for Analyzing Computing Systems / [V.I. Hahanov, W. Gharibi, S.V. Chumachenko, E.I. Litvinova] // Computer Science & Information Technology (CS & IT). – 2014. – P. 73-81. DOI: 10.5121/csit.2014.41108

12. Big Data Driven Cyber Analytic System / [V. Hahanov, E. Litvinova, W. Gharibi, S. Chumachenko] // IEEE International Congress on Big Data. – New York, NY, USA. – 27 June – 2 July 2015: proceedings. – IEEE, 2015. – P. 615-622. doi: 10.1109/BigDataCongress.2015.94.

13. QuaSim – Cloud Service for Digital Circuits Simulation / [I. Hahanov, I. Iemelianov, W. Gharibi, T. B. Amer] // *2016 IEEE East-West Design & Test Symposium (EWDTS)*. – Yerevan, Armenia. – 14-17 October 2016: proceedings. – IEEE, 2016. – P. 1-8. doi: 10.1109/EWDTS.2016.7807667.

14. Адамов О. С. Моделі і методи захисту кіберпростору на основі аналізу великих даних з використанням машинного навчання : дис. канд. техн. наук : 05.13.05 "Комп'ютерні системи та компоненти" / Адамов Олександр Семенович; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків, 2019. – 243 с. http://openarchive.nure.ua/handle/document/11978