УДК 658.512.011: 681.326: 519.713

БЛОКЧЕЙН ІНФРАСТРУКТУРА ДЛЯ ЗАХИСТУ КІБЕРСИСТЕМ

АДАМОВ О.С., ХАХАНОВ В.І., ЧУМАЧЕНКО С.В., АБДУЛЛАЄВ В.Г.

Пропонується блокчейн технологія і математичний апарат створення інфраструктури програмно-апаратних телекомунікаційних інформаційних кіберфізичних систем (КС), орієнтована на захист від несанкціонованого доступу до сервісів, визначених у специфікації системи, шляхом проникнення через легальні інтерфейси взаємодії компонентів, що мають уразливості. Інфраструктура захисних сервісів створюється разом з кіберсистемою і супроводжує останню протягом всього життєвого циклу, обслуговуючи всі наступні модифікації КС, і сама постійно підвищує свій інтелект шляхом поповнення історії та бібліотек конструктивних і деструктивних компонентів.

1. Вступ. Практика використання топ-технологій

Високі витрати на дослідження і розробки від Amazon, Apple, Baidu, Google, IBM, Microsoft і Facebook стимулюють створення оригінальних патентованих рішень в області Deep Learning і Machine Learning, серед яких слід відзначити: Amazon Alexa, Apple Siri, Google Now, Microsoft Cortana. Компанія Gartner Inc. впевнена, що інструменти для глибокого навчання становитимуть 80% стандартних засобів для вчених. Сьогодні вже на сайтах компаній стають доступними технології і дані про наукові дослідження: Amazon Machine Learning, Apple Machine Learning Journal, Baidu Research, Google Research, IBM AI і Cognitive Computing, Facebook Research.

Впровадження 5G-технології телекомунікацій (рис. 1) в найближче десятиліття надасть ринку очікувані інноваційні рішення з безпеки, масштабованості і продуктивності глобальних мереж і з'єднань в транспорті, IoT, індустрії, охороні здоров'я.

Gartner Inc. прогнозує, що до 2020 року 3% мережевих провайдерів послуг мобільного зв'язку запустять комерційні мережі в 5G-форматі, що забезпечить якісно нові умови повсюдного впровадження телекомунікацій для масштабованої глобалізації сервісів: IoT, cloud-transport control, UHD-телебачення. Лідерами 5G-впровадження в 2017-2018 році виступають: AT & T, NTT Docomo, Sprint USA, Telstra, T-Mobile і Verizon. Технологія 5G є ультраширокополосний мобільний зв'язок в міліметровому діапазоні для Massive M2M транзакцій в реальному часі з допустимими для управління затримками (1мс), при одночасному підключенні близько 10 млн пристроїв на 1 км кв. 5G використовує технологію множинного доступу з поділом променя (Beam Division Multiple Access – BDMA) для взаємодії базової станції з мобільними пристроями. Бездротова стільникова архітектура 5G забезпечує пропускну здатність 10-50 Гбіт / с в міліметровому діапазоні частот 30-300 ГГц для додатків UHD відео і створення віртуальної реальності [4]. Інноваційна технологія 5G характеризується використанням: масиву приймально-передавальних антен Massive MIMO, мережі Cognitive Radio, організацією безпосереднього зв'язку D2D для IoT, створенням мережі радіодоступу, як хмарної послуги (radio access network as a service) і хмари віртуальних мережевих функцій (network function virtualization cloud – NFV).

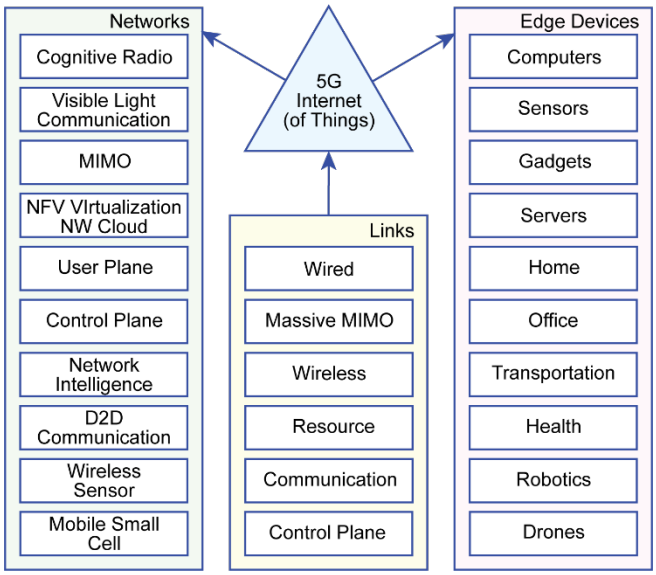

Рис. 1. Три складових технології 5G

Hype cycle, з незрозумілих причин, не розглядає дві істотних для людства абсолютно зелені і мультимільярдні технології, пов'язані з кіберсоціальним комп'ютингjv: Digital Humanity і Smart Cyber Digital State. Вони додані авторами публікації в Gartner's Table for Emerging Technologies, як запускаються інновації першої фази (innovation trigger), реалізація яких очікується через 5-10 років.

Digital Humanity – оцифроване людство передбачає точну цифрову ідентифікацію особистості з природничими біометричними параметрами (відбитки пальців, сканування обличчя, очі і ДНК), що виключають паперові носії інформації, пластикові карти, посвідчення, дипломи та паспорти в планетарному масштабі. Цифровий ідентифікатор дає можливість делегувати позиціонування кожної людини в часі і просторі хмарного сервісу, який знімає всі проблеми, пов'язані з кіберфізичним аналізом нелегітимних дій кожного індивідуума. Наслідком сталого

розвитку цифрового людства в рамках зеленого інтернету речей для створення розумного світу [5] є багатомільярдна економія витрат на виробництво і використання паперових документів, збереження лісів і планетарної екології. Платою за отримання згаданих дивідендів є витрати на створення електронної інфраструктури для цифрової аутентифікації кожної особистості, процесу або явища в часі і просторі. Green IoT – кіберфізична культура людської діяльності, спрямована на забезпечення якості життя людей і збереження екології планети, енергії, ресурсів і часу. Компонентами IoT є: Identification, Sensing, Controlling, Communication, Cumputation, Sevices Intelligent, Digital Infrastructure. Розумний світ (smart world) надає кожній людині сервіси від: розумних пристроїв (watches, mobile phones, computers), розумного транспорту (aircrafts, cars, buses, trains), розумної інфраструктури (homes, hospitals, offices, factories, cities, states), розумної цифрової освіти (school, university).

Світ без посередників – це є інноваційний технологічний уклад прямих телекомунікаційних контактів кожної людини з будь-яким суб'єктом на планеті, завдяки використанню кіберфізичних сервісів. Якщо людство вирішиться на знищення корупції в глобальному масштабі, воно зробить це за допомогою Blockchain [6]. Це є децентралізована криптографічна прозора технологія зберігання та обміну даними про виконані транзакції, яка здійснює пряму взаємодію бізнесменів або суб'єктів без довірчих юридичних посередників в рамках IoT-сервісу. Проте без легітимного визнання Blockchain з боку державних структур дана технологія є поки ресурсовитратним експериментальним антикорумпованим анклавом в кіберпросторі даних і транзакцій, узаконених владою.

Журнал IEEE Spectrum [7] опублікував тематичну добірку статей про технології Blockchain під девізом: "In cryptography we trust". По суті, технологія відкидає всіх "довірених" посередників: банкірів, багатомільйонну армію державних чиновників при здійсненні угоди між двома сторонами. Третя сторона-посередник завжди є надлишковою, яка зменшує прибуток бізнесменів-виробників, ускладнює транзакції і, що найголовніше, – є єдиним джерелом корупції на планеті. «Прагнення людей до секретності робить їх дурними: не видно ні поганих, ні хороших результатів. Julian Paul Assange».

Технологія Blockchain (зокрема, bitcoin) являє собою кіберфізичний метричний хмарний криптозахищені комп'ютинг прозорого моніторингу та довірчого управління транзакціями в розподілених blockchain data (рис. 2).

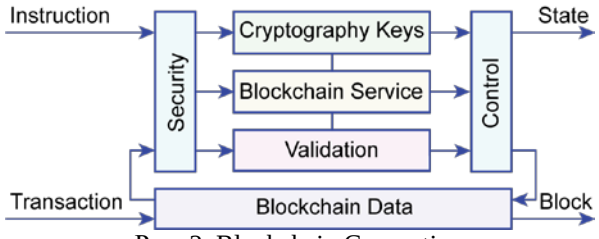

Рис. 2. Blockchain Computing

Технологія, спочатку запропонована Satoshi Nakamoto (2009), сьогодні стійко розвивається як розподілений в просторі і часі довірчий комп'ютинг з ненадійних компонентів: Ethereum Virtual Machine (2013, Vitalik Buterin); Microsoft blockchain додатки на хмарі Azure; IBM і Intel відкриті ресурси Hyperledger. За даними Blockchain.info в проект Bitcoin сьогодні вже залучено понад 375 000 чоловік (China, Eastern Europe, Iceland, Venezuela). Криптовалюта стає вагомозначущим універсальним посередником між продавцем і покупцем для оцінювання соціальної значущості товарів і послуг. Ринкова капіталізація Bitcoin зросла до більш ніж 137 мільярдів доларів, а вартість біткойнів у квітні 2018 року дорівнювала 8000 доларів. Приріст вартості криптовалют за рік склав 1000 доларів.

Тому замінити паперові грошові знаки на віртуальні (цифровий код) буде тривіально просто, оскільки папір не може постояти за себе. Труднощі виникнуть при заміні мільйонів чиновників, які виконують роль посередників-довірителів, на комп'ютингові хмарні системи управління. Чиновники мають владу, зброю і будуть стояти насмерть для збереження посередництва у корумпованому в розподілі грошей і ресурсів (рис. 3).

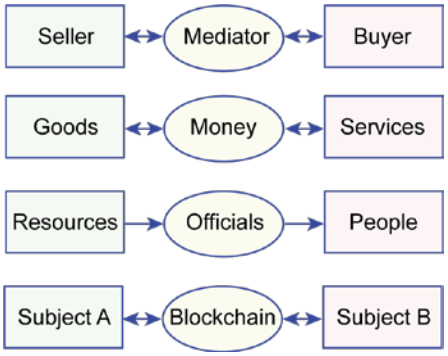

Рис. 3. Сфери застосування Blockchain Computing

Область застосування технології Blockchain – кіберфізичні процеси і явища, що уражені корупцією, завдяки наявності посередників, які не можуть бути дійсно довірчими, зважаючи на людську слабкість

– привласнити чуже, якщо відсутнє покарання. Фактично можна і потрібно будувати Blockchain довірчі системи для відкритого управління наукою, освітою, туризмом, транспортом, фінансами, соціумом, медициною і кадрами. Ethereum є blockchain (bitcoin) world-комп'ютинг, який може замінити Facebook, Twitter, Uber, Spotify, будучи невразливим для цензорів і прозорим щодо процесів, що відбуваються, а також довго працювати при відсутності людей, які його створили.

Недоліки Blockchain комп'ютинга: 1) багаторазове дублювання даних в розподіленій мережі; 2) відкритість цінних даних, патентів і кодів, яка зруйнує частину компаній; 3) високі витрати на створення інфраструктури, орієнтованої на Blockchain; 4) запеклий опір державних структур впровадженню системи морального розподілу ресурсів. "Money is not the root of all evil. Equity is the root of all evil ", Joel Monegro. Іншими словами, рівність у злиднях є причина деградації соціуму.

2. Blockchain Computing

Біткойн був створений як незалежна технологія моральної оцінки соціальної значущості результатів діяльності людей, спрямованої проти надмірності, несправедливості і корумпованості традиційної фінансової системи. Зростання соціальної значущості паралельної валюти створює серйозну конкуренцію посередницьким і фінансовим інститутам, які в кінцевому підсумку будуть деструктурувати. Теза «In cryptography we trust» не залишає місця посередникам, банкірам, довіреним особам і іншим третім сторонам, які суттєво уповільнюють всі процеси людської діяльності, зменшуючи прибуток і ускладнюючи транзакції [7].

Біткойн замінює сервіси, що надаються сьогодні посередниками, на криптографію і виконуваний код. Біткойн і інші криптотранзакції замінюють договірні угоди з банком і з іншими людьми на розподілену і захищену базу даних, яка називається блокланцюжком. Процес верифікації, за допомогою якої володіння токеном біткойнів буде переходити від однієї людини до іншої, довіряється мережі комп'ютерів.

Через 9 років після створення першого блокчейна в формі криптовалюти люди досить успішно застосовують його до соціальних процесів і явищ, де можна замінити посередників на blockchain. Включивши мінімальну фантазію, можна запропонувати тисячі проектів для заміни на blockchain завжди дорогих посередників між продавцем і покупцем товарів і послуг: пропонувати безпосередньо розваги, подорожі, атракціони, телебачення, фільми, концерти, спортивні змагання, квитки на транспорт. При цьому не залишиться місця не тільки банкам, але і таким сервісам, як Uber, Netflix.

Згадані додатки є прикладами послуг, побудованих на Ethereum blockchain платформі, яка дистанційно виконує software на розподіленій комп'ютерній системі, названій Ethereum Virtual Machine. Ethereum blockchain кіберпростір, що має свою криптовалюта (ethers), є найбільш відкритим для проведення експериментів з боку численних груп дослідників, які хочуть змінити світ. Лідери IT-індустрії також грають на стороні blockchain. Microsoft пропонує своїм клієнтам інструменти для експериментів з blockchain в хмарі Azure. IBM, Intel та інші компанії підтримують blockchain з відкритим вихідним кодом в проекті Hyperledger, метою якого є створення архітектур для бізнес-орієнтованих blockchain. Тим часом багато хто з найбільших банків створили власну версію blockchain, намагаючись очолити успішний розвиток і просування технології. Проте проекти blockchain ще не революціонізували жодну галузь, як того б хотілося її творцям. Згідно з даними Blockchain.info, криптовалюта використовується в співтоваристві, що складається з 375 000 чоловік з інтегральним рівнем cryptospace-капіталізації, рівному 400 мільярдів доларів [https://www.youtube.com/watch?v=UaCAHbOQQag &t=]. Але долари інвесторів незмінно дорожчають, а маси нових пропозицій виникають з невичерпного джерела blockchain, більшість з яких поки не сприймається бізнесом і науковим співтовариством як безальтернативне майбутнє.

У 2009 році хакер, на ім'я Сатоші Накамото, який вважається основоположником релігії bitcoin, оприлюднив першу цифрову валюту. Технологія працювала за принципом: гроші – це інструмент обліку і абстрагування вартості товарів і послуг при здійсненні операцій. Гроші є історичним метричним посередником для еквівалентного обміну товарами і послугами. Володіння фізичними знаками або монетами рівнозначно володінню матеріальними товарами або послугами. Якщо замість грошових знаків створити таблицю учасників закритого співтовариства, де будуть прописані рахунки кожної людини, то фізичні банкноти і монети стануть непотрібними. Банки вже частково трансформували фізичну валюту в цифрові записи обробки транзакцій в їх закритих системах. Біткойн завершив перетворення, створивши універсальний цифровий ledger (бухгалтерську книгу), так званий blockchain, де зміни можуть бути зроблені тільки шляхом додавання нового запису в кінець блокового ланцюжка. Blockchain біткойнів, на відміну від бухгалтерських книг, підтримуваних традиційними фінансовими

установами, реплікірується на мережевих комп'ютерах і доступний для кожного учасника закритої або відкритою мережі. Клас учасників мережі, які називаються майнер, відповідає за виявлення запитів на транзакції від користувачів, їх перевірку і додавання нових блоків в blockchain.

Валідація виконує перевірку спроможності покупця, який володіє біткойнами в своїй транзакції, які він не витратив в іншому місці. Власність в blockchain ланцюжку біткойнів визначається парою криптографічних ключів. Перший, відкритий ключ, знаходиться в блокчейні для всіх учасників. Другий є закритим ключем, який власник зберігає в безпеці. Два ключі знаходяться в спеціальному математичному відношенні, яке робить їх корисними для цифрового підпису транзакцій. Ось як це відбувається: користувач формує повідомлення, об'єднує його зі своїм особистим ключем, виконує певні математичні обчислення для отримання довгого числа. Будь у кого є вихідне повідомлення і відповідний відкритий ключ може зробити деякі власні обчислення, щоб довести – довге число було створено за допомогою закритого ключа. У біткойнів транзакції підписуються закритими ключами, які відповідають відкритому ключу, пов'язаному з матеріалами, що витрачаються монетами. І коли транзакція обробляється, цим монетам присвоюється новий відкритий ключ. Головна роль blockchain-мінерів полягає в забезпеченні незворотності нових транзакцій, що робить їх остаточними і захищеними від несанкціонованого доступу з боку хакерів. Біткойн не має централізованої влади для дотримання правил. Майнери працюють анонімно в усьому світі, в просторі різноманітності культур, правових систем і нормативних зобов'язань. Тому немає простого фізичного способу привернути користувача-порушника до відповідальності. Щоб забезпечити легітимну поведінку людини, Bitcoin використовує схему, названу доказом виконаної роботи, яка відповідає відкритому ключу, пов'язаному з матеріалами, що витрачаються монетами.

У відкритій часової мережі майнери запускають біткойн-код, отримують нові транзакції і збирають їх для створення нового блоку. Майнер конкурують один з одним. Перший, хто створить дійсний блок, отримує оплату в біткойні за цю послугу. Важливо, щоб всі мінери в мережі біткойн мали одну і ту ж копію блок-ланцюга, а всі зміни і транзакції незворотні. Щоб синхронізувати всіх мінерів, необхідно дороге програмне забезпечення, великі обчислювальні і енергетичні потужності для додавання дорогих за витратами змін в нових блоках.

Будь-який майнер, який намагається додати новий блок, повинен надати криптографічний доказ шляхом перетворення нового блоку за допомогою декількох обчислювально складних раундів визначення хеш-функції. Blockchain вимагає, щоб отриманий хеш починався з певної кількості нулів. Перший майнер, який знаходить задовільний хеш, оголошує новий блок іншим колегам, які перевіряють код і додають його до повної версії blockchain, яку вони записують на своїх комп'ютерах. За виконання даної роботи майнер отримує винагороду, а також гонорари за волонтерський видобуток «корисних копалин». Приклад: є замок, який потребує ключа для закриття, і є безліч ключів в розпорядженні користувача. Завдання полягає в пошуку правильного ключа за матеріальні стимули, який потім слід залишити в замку,

Біткойн-майнери інвестують ресурси в мережу, яку вони обслуговують, в частині електроенергії та комп'ютерного обладнання. Тому вони не схильні пошкодити валюту будь-якими діями або зовнішніми атаками, які можуть поставити під сумнів цілісність біткойнів і їх валідність. Успішність атак у міру зростання мережі зменшується, оскільки вартість зміни вмісту старих блоків збільшується з кожним новим блоком, який додається в ланцюжок. Наприклад, другий блок містить хеш тільки першого. Будь-які зміни в старих блоках приведуть до недійсним хеш для всіх наступних компонентів. Отже, неможливо вставити фіктивні модифікації в попередній блок без повторення всієї роботи, яка була виконана після створення цього блоку. Конструкція блокування в кінці ланцюга залежить від усіх замків, які були зроблені перед нею. Тому зміна одного замка в середньому блоці ланцюжка означає необхідність пошуку нових ключів для кожного блоку після нього. Якщо є користувач, що володіє надпотужними обчислювальними ресурсами, то хакерська атака зі зміни записів можлива.

Сатоші створив першу життєздатну однорангову цифрову валюту. Але головне, він вирішив більше загальну проблему консенсусу, яка протягом десятиліть дратувала соціально-комп'ютерних вчених. Біткойн протягом останніх десяти років надійно стимулює до активності мережу потенційно нечесних анонімних учасників для чесної обробки транзакцій і забезпечення єдиної версії всіх подій. Результатом є постійно зростаючий ланцюжок даних, який будь-який користувач інтернету може перевіряти і доповнювати, а також той, що сьогодні є неймовірно захищеним від атаки.

Blockchain система може бути корисною набагато більше, ніж просто грошові відношення без посередників. Після успішного біткойн-дебюту дослідники почали генерувати інші ринковоорієнтовані додатки на блокчейн-платформі. Коли мінери перевіряють транзакції, вони запускають невеликі програми, які обробляють дані і надають «так-ні» експертний висновок за запитом транзакції. Вони можуть запускати більш складні програми, такі як соціальні мережі, онлайн-форуми, управління соціальними групами і державами. Молодий програміст Віталік Бутерін розробив абсолютно новий блокчейн під назвою Ethereum. Мета проекту – поширити біткойн на інші сфери людської діяльності. Ethereum використовує блок-ланцюг, у якого є своя валюта, що називається ефірами. На відміну від Bitcoin, Ethereum використовує транзакції, які є мініпрограмними або інтелектуальними контрактами з необмеженим ступенем складності. Користувачі можуть взаємодіяти з програмами, завантажуючи в них транзакції з інструкціями, які обробляють мінери. На практиці це означає, що будь-який користувач може вбудувати програму в транзакцію з упевненістю, що вона залишиться там незмінною і доступною для всіх учасників. Теоретично Ethereum може замінити Facebook, Twitter, Uber, Spotify або будь-яку іншу цифрову службу новими версіями, які будуть недоступні для цензорів і прозорі для всіх учасників, працюючи нескінченно в часі при відсутності розробників. Дивно, що можна помістити комп'ютерну програму в Ethereum мережу, де всі учасники в системі можуть домовитися про те, що і коли буде відбуватися в мережі. Засновник Ethereum, Joseph Lubin, тепер запускає Consensys – Brooklyn-based інкубатор для децентралізованих додатків. Фактично можна створювати інфраструктури для накопичення та обміну будь-якими товарами і послугами, організовуючи спеціальні і універсальні мережі на основі blockchain-культури.

Обліковий запис або Permissioned Ledger. Паралельно з Ethereum-практикою використання технології blockchain для створення глобального комп'ютера, існує зворотна тенденція, пов'язана з реалізацією закритої і контрольованої мережі Сатоші. Група фінансових інститутів (Barclays, Goldman Sachs і JP Morgan) в 2014 році сформувала консорціум під назвою R3 для підвищення ефективності платежів між банками шляхом впровадження blockchain. Стало зрозуміло, що відкрита структура blockchain (біткойнів і ефіріум) суперечить їхнім потребам: анонімність користувачів, які на відкритих блокових ланцюгах представлені буквено-цифровими загальнодоступними адресами, без їх автентичності суперечить банківському законодавству в Сполучених Штатах і в інших країнах. Банкам важливо знати, хто є їх клієнтами і контрагентами. Фінансові установи юридично зобов'язані захищати дані про вкладників і контролювати їх транзакції за міждержавними і регіональними лініями. Публічні blockchain реплікують запис транзакції на кожному комп'ютері в мережі, що робить неможливим обмежити зберігання даних про транзакції при використанні технології блокового ланцюжка в банках.

В результаті з'явився підхід «дозволеної книги» в технології blockchain, де відомі ідентифікатори людей, що додають блоки, а дані в системі доступні тільки для окремих призначених осіб. Оскільки право створювати нові блоки визначається людьми, які запускають код, а не випадково, то немає необхідності в перевірці валідності криптовалюти при оплаті. Така система (наприклад, Corda) використовується в ситуаціях, коли всі учасники блокового ланцюга мають певний ступінь довіри, але хочуть змоделювати послуги нейтральної третьої сторони (банків) при регулюванні міжнародних банківських переказів.

Підхід «дозволеної книги» поширюється за межі банків в інші галузі, які є охоронцями конфіденційних даних клієнтів. Багато з цих проектів побудовані за допомогою інструментів, що надаються Hyperledger проектом з відкритим вихідним кодом, організованим фондом Linux і підтримуваним великими технологічними фірмами. Hyperledger створює продукти для компаній, які хочуть працювати зі смарт-контрактами, але не наважуються використовувати відкриті blockchain (Ethereum, Bitcoin) мережі. «Користувачі повинні приймати нормативні вимоги, що пред'являються до таких організацій, як банки, страхові компанії і галузі охорони здоров'я. Останні не можуть дозволити собі ризик і невизначеність, які супроводжують відкриті системи» (Джонатан Леві, автор Hacera-системи управління доступом до блокових ланцюгів).

З'єднання смарт-контрактів і blockchain вимагає підтримки технологій для вирішення цілої низки проблем. Blockchain мережі не можуть зберігати структури великих даних, які вимагають реплікації. Наприклад, неможливо поширювати потокове відео за блочним ланцюжком, що містить мільйони вузлів. Ще одна проблема смарт-контрактів полягає в тому, що blockchain не може моніторити реальний світ, тільки віртуальний. Наприклад, якщо розумний контракт - система страхування польотних квитків, він повинен знати, коли літак злетить і приземлиться. Тут blockchain поки не має функцій запиту

відповідних веб-сайтів про видачу польотної інформації, яку він повинен семантично розшифрувати. Для цього потрібні розумні доповнення до blockchain у вигляді хмарних сервісів або програмних додатків. Розробники повинні створювати blockchain для зберігання і доступу до даних, захищених від уразливості, цензури і деструктивних проникнень. Проблема зберігання даних може бути вирішена за допомогою розподілених децентралізованих хмарних систем Labs Interplanetary Database або Storj Labs. Вони дозволяють користувачам здавати в оренду зайвий простір на своїх жорстких дисках. Такі розподілені мережі придатні для системи інтелектуальних контрактів на основі blockchain, де дані будуть надмірно зберігатися на безлічі комп'ютерів по всьому світу і завжди будуть доступні цензурі.

Імпорт даних в blockchain здійснюється в режимі реального часу «оракулами», які отримують оплату за надійний запит джерел даних і подачу їх на смарт-контракти в блок-ланцюжку. Наприклад, оракул Town Crier призначений для введення даних в блок-ланцюжок з надійного джерела на основі довірчого криптографічного програмного забезпечення на процесорах Intel. Отже, технологія blockchain повинна доповнюватися розумними програмними або хмарними сервісами, які будуть враховувати специфіку конкретної галузі людської діяльності.

Де взяти гроші для реалізації blockchain технології, щоб заплатити за техніку, сервіси та глибокі наукові дослідження? Створення нових функцій, алгоритмів і архітектур передбачає візуалізацію або знищення цінних даних, на основі яких виживають багато підприємств? Ethereum довіряє дані тим людям, які створили blockchain. Компанія не може вийти з рамок бізнес-моделі, яка збирає і продає товари і послуги, має історію покупок і дані про місцезнаходження партнерів. Компанія blockchain не може також покладатися на обмежене володіння своєю інтелектуальною власністю, оскільки програми на відкритому блокчейні доступні для загального огляду. Вже з'явився потенційний механізм фінансування підприємств з прив'язкою до blockchain, названий пропозицією монет Initial coin offering (ICO), який виявився прибутковим, хоча і юридично сумнівним. Групи, що фінансують проекти за допомогою ICO-залучення інвестицій у вигляді продажу користувачам фіксованої кількості нових криптовалют, розробляють розумні контракти на основі використання монет для покупки додатків. Ці групи створюють монети до запуску проекту, які продаються на відкритому ринку. Наприклад, жетони для проїзду в метро випускаються і продаються до поїздки. Це дає можливість, замість пошуку інвестора, надрукувати масу монет (власну валюту) для продажу населенню, які потім можуть реалізовуватися за цінами, обумовленими вартістю поїздки на метро. Сьогодні понад півмільярда доларів обертаються в blockchain-компаніях шляхом продажу токенів, які в останні кілька місяців стали помітно зростати в ціні за рахунок появи нових інвестиційних пропозицій. Blockchain проект під назвою Tezos недавно встановив рекорд, зібравши більше 200 мільйонів доларів з ICO, ITO (продаж токенів). Підприємці blockchain насправді демонструють скупість і жадібність фінансових інститутів, що використовують страндартні валюти, підтримувані урядом. Коли гроші починають текти в інший бік, чиновники стають однаково незговірливими щодо громадськості, з якої вони вийшли. Деякі експерти стверджують, що ICO, як новий клас інвестиційного інструменту, настільки ж руйнівна, як і фінансовані за даною схемою додатки. «Гроші не є коренем усього зла. Рівність є коренем усього зла», говорить Joel Monegro, засновник фонду Placeholder, орієнтованого на технології blockchain. Його аргумент полягає в тому, що надання засновникам і співробітникам акцій компанії спонукає їх накопичувати багатство, а не використовувати його для поліпшення своїх потреб. Монета, призначена для додатків, є не тільки фінансовим інструментом, а й засобом доступу до технологій. З цього випливає, що чим більше людей користуються послугою, тим більшим буде соціальний попит на токен, необхідний для доступу до цієї послуги. «Стимул компанії полягає не в отриманні більшого прибутку, а в отриманні більшого використання токена на основі масовості реалізації послуги серед населення». Сполучені Штати, ймовірно, будуть забороняти ICO-технологію, оскільки багато хто з розглянутих токенів потрапляють в категорію цінних паперів і повинні підкорятися існуючим правилам. Необхідно, щоб Bitcoin і Ethereum функціонували в більших масштабах, а підприємствам слід децентралізовувати більше криптовалюти і забезпечувати конфіденційність даних. З огляду на величезні суми вкладених в blockchain грошей, необхідно залучати нових користувачів,

Децентралізація валют в глобальному масштабі на основі впровадження в практику bitcoin є моральною альтернативою розвитку людства, яка поки що не може промоделювати майбутнього. Однак з постулатів і визначень поступово складається картина blockchain культури, представлена на рис. 4:

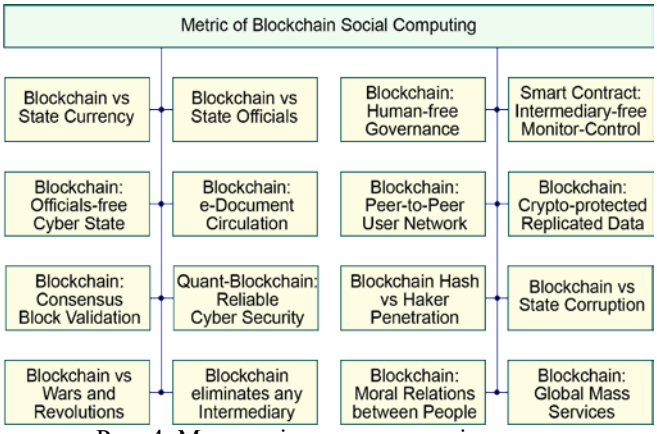

Рис. 4. Метричні параметри соціального blockchain-комп'ютинга

1) Криптовалюти здатні конкурувати з національними валютами і мирно захоплювати фінансову, політичну, економічну, законодавчу владу тотально або в окремих сегментах людської діяльності. 2) Кожна соціальна група, яка має спільні інтереси, може створювати власну криптовалюту для обміну певними товарами і послугами без використання зовнішніх валют. 3) Бартерні відносини при соціалізмі всередині закритої соціальної групи: «ти – мені, я – тобі» є фізичний прихований від суспільства прообраз криптовалюти без використання стандартних грошових знаків. 4) Будь-які корумповані, завжди закриті співтовариства довіряють один одному людей, використовують власну валюту для обміну цінностями: придбання посади, земельної ділянки, вступ до вишу, складання іспитів. 5) Випуск компанією цінних паперів, акцій рівносильний емісії токенів, криптовалюти і bitcoin. 6) Приватизація частини державної власності через випуск акцій аналогічна створенню тимчасової мережі, де учасники-акціонери можуть купувати і продавати один одному свої частки власності. 7) Позитивізм створення тимчасових blockchain мереж полягає у виключенні будь-яких посередників при укладенні розумних контрактів між учасниками закритого співтовариства. Посередниками виступають державні структури, приватні організації, банки і чиновники, які виробляють товари та послуги, що суттєво збільшують накладні витрати на ведення бізнесу. 8) Наявність метрики (криптовалюти) вимірювання соціальної значущості товарів та послуг в замкнутій мережі користувачів є умовою її існування. 9) Blockchain мережа, як система, має на меті підвищення якості життя та збереження екології планети шляхом морального human-free управління соціальними процесами без участі посередників для метричного розподілу матеріального і / або винагороди на основі вичерпного моніторингу соціальної значущості і верифікованих транзакцій, розумних контрактів. 10) Blockchain мережа масштабується в кібердержаву, де суб'єктами виступають компанії і організації, метрично розподіляють на основі консенсусу гроші платників податків без участі посередників. Кібердержава отримує частину прибутку від суб'єктів на розвиток і забезпечення життєдіяльності соціальної системи. 11) Смарт-контракт – метрично розподілені на основі консенсусу гроші платників податків без участі посередників. Кібердержава отримує частину прибутку від суб'єктів на розвиток і забезпечення життєдіяльності соціальної системи. 12) Смарт контракт – кіберсоціальна система електронних intermediary-human-free відносин між покупцем і продавцем товарів і послуг, реалізована у вигляді криптозахищеного програмного коду, що має на меті достовірне виконання сторонами договірних умов на основі вичерпного моніторингу процесу виконання зобов'язань і вироблення адекватних актюаторних впливів на компоненти blockchain-інфраструктури. 13) Електронний документообіг – кіберсоціальна система електронних intermediary-human-free відносин між працівниками компанії на е-інфраструктурі, реалізована у вигляді криптозахищеного програмного коду, що має на меті достовірне виконання сторонами наказів і розпоряджень шляхом вироблення адекватних актюаторних впливів на основі вичерпного моніторингу процесу виконання документа. 14) Blockchain комп'ютинг – обчислювальний процес в замкнутій розподіленій кіберсоціальній часовій комп'ютерній мережі, призначеній для виконання смарт-контрактів і збереження реплікування криптозахищених ланцюжків записів про транзакції на основі human-free моніторингу і консенсусної валідації кожного нового блоку з метою створення толерантних метричних довірчих відносин, без посередників, між ненадійними учасниками мережі. 15) Квантовий комп'ютинг не тільки створює засоби для успішного проведення хакерських атак на сучасні blockchain-інфраструктури, але в більшій мірі він надасть нові технології надійного кіберзахисту блокових ланцюжків шляхом впровадження логіки квантового змішування, що дозволяє стискати простір і час в структурах даних. 16) Хеш-функція являє собою цифрову сигнатуру фіксованої довжини для бажаної довгої кінцевої вхідної послідовності бітів, отриману в результаті послідовного застосування односпрямованого функціонального xor-шифрування цифрових блоків фіксованої довжини, при відомому початковому ключі. 17) Держава є посередник у відносинах між громадянами. Носіями

державності виступає армія посередників-чиновників. Посередник не є виробником товарів і послуг. Він привласнює товари і послуги, які не належать йому, а потім продає їх всім громадянам. Корупція існує поки є державна власність. Знищити корупцію означає знищити посередників і / або державну власність шляхом їх заміни на blockchain-інфраструктуру прямих відносин між громадянами. Інакше, створюється моральна кібердержава, де функції посередника у відносинах між громадянами виконує blockchain мережа.

Інтегральне уявлення кіберфізичної системи blockchain-комп'ютинга зображено на рис. 5.

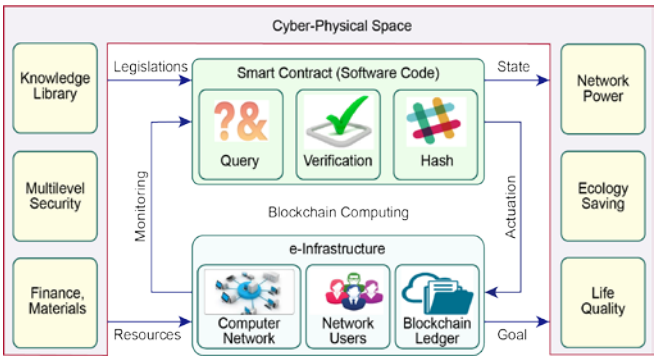

Рис. 5. Кіберфізична система blockchain-комп'ютинга

Система характеризується human-free управлінням процесами виконання розумного контракту на основі цифрового моніторингу сенсорів, пов'язаних з транзакціями товарів, послуг і фінансів, а також з формуванням захищених blockchain-структур даних на всіх комп'ютерах розподіленої мережі.

«Blockchain і цифрові активи, такі як Bitcoin і Ether, революційно оцифровують області людської діяльності, включаючи освіту, промисловість, фінансові послуги, охорону здоров'я, уряд, менеджмент, енергетику, нерухомість і суспільство" [12]. Динаміка вартості bitcoin почалася з цифри 936 доларів і досягла до середині грудня 2017 – 19 500 доларів. Однак за два тижні до кінця грудня, криптовалюта зменшилася на 30 % – 14 100 доларів. Тому при покупці криптовалюти слід користуватися правилом – вкладайте рівно стільки грошей, скільки вам не шкода втратити.

Квантові блокчейни можуть функціонувати як машини часу і протистояти атакам хакерів за допомогою квантових комп'ютерів. Quantum Blockchains Could Act Like Time Machines [13].

З'єднання двох технологій: квантового комп'ютинга і блокчейна може привести до створення Q-Blockchain Systems (QBS), непроникних для злому з боку квантових комп'ютерів. Важливо відзначити, що Q-Blockchain функціонує як машина часу, яка здатна впливати на власне минуле.

Blockchain являє собою базу даних, в якій зберігаються записи про минуле системи, наприклад, історія фінансових або інших транзакцій, які були узгоджені з кожним вузлом мережі без централізованого управління. Найбільш відомим застосуванням Blockchain є криптовалюта біткойн, проте існує безліч компаній і дослідників, які пропонують інші можливості для використання даної технології. За словами Del Rajan, фізика-теоретика з Новозеландського Університету в Веллінгтоні, очікується, що до 2027 року на основі технології Blockchain можна буде зберігати 10 відсотків світового ВВП. Кіберкультуру Blockchain очікує плідна зустріч з іншою сучасною технологією – квантовим комп'ютингом, що використовує квантові біти або кубіти, які через сюрреалістичну природу квантової фізики можуть перебувати в стані суперпозиції, коли X = {0,1}. Суперпозиція бітів в кубіті дає можливість одночасно виконувати два обчислення, а в загальному випадку – 2**n операцій на n кубітах. Теоретично квантовий комп'ютер з 300 кубітами здатний виконати більше обчислень в одну мить, ніж число атомів у видимій частині Всесвіту. Потужний квантовий комп'ютер здатний успішно перемогти класичну криптографію, в тому числі і сучасний захист Blockchain. Однак відбивання технологій Q-computing + Blockchain = Q-Blockchain може конструктивно протистояти спробам злому з боку квантових комп'ютерів.

Q-computing використовує квантове переплутання в просторі (Quantum Entanglement in Space), яке визначається взаємним впливом двох і більше часток один на одного, інваріантним до відстані – spooky action at a distance, за словами Альберта Ейнштейна. Переплутання в Q-computing означає згортку простору в одну точку.

Дізрапторна інновація Q-Blockchain визначається змішуванням або зв'язуванням квантових частинок в часі (Quantum Entanglement in Time), яке формується взаємним впливом двох і більше часток один на одного, інваріантним до будь-якої часової відстані між ними. Тут квантове переплутання означає згортку часу в одну точку.

Blockchain формує записи в блок-ланцюжки даних, які мають криптографічні посилання, задані в хронологічному порядку. Якщо хакер спробує змінити запис конкретного блоку, то криптографічний алгоритм анулює всі наступні блоки після зламаного.

Q-Blockchain формує записи в блок-ланцюжку фотонів або квантів, які переплутані або пов'язані між собою в хронологічному порядку, в часі. Тут записи

формують квантовий блок-ланцюжок, де фотони, які кодують кожен блок, передаються всіма компонентами мережі квантових комп'ютерів. Q-Blockchain переплутання пов'язує всі фотони в часі. Інакше, записи в Q-Blockchain часового ланцюжку теперішньої і минулих транзакцій закодовані в єдиному квантовому стані, що означає згортку часу в одну точку.

Хакер не може втручатися в запис блок-ланцюжків минулого, оскільки відповідні фотони більше не існують в теперішньому часі – вони вже переплутані. У кращому випадку хакер може успішно змінити фотон останнього блоку (це зробить його недійсним, повідомляючи всім іншим, що він зламаний). Така атака є менш суттєвою, ніж стандартний випадок, коли хакер має можливість змінити будь-який блок в часовому ланцюжку.

Квантова заплутаність в часі означає, що вимір останнього фотона в блоці впливає на перший фотон цього блоку в минулому перед тим, як його виміряли. Measuring the last photon in a block influences the first photon of that block in the past before it got measured. По суті, поточні записи в квантовому блоковому ланцюжку не просто пов'язані із записом минулого, а швидше з записом в минулому, якого більше не існує. «Проект в певному сенсі може розглядатися як квантова машина часу», – говорить автор Метт Виссер (Matt Visser), фізик-теоретик з Веллінгтона.

3. Системні проблеми, пов'язані з «проникненням» і «вразливістю»

Поняття, що визначаються словами «проникнення» і «вразливість», є взаємодоповнюючими один одного. Якщо є вразливість, то в неї, як у дірку, можливе проникнення деструктивності, яка вписується в функціональність кіберсистеми. Вірно і зворотне, якщо зафіксовано проникнення, то воно сталося внаслідок наявності в системі уразливості (дірки). Проблема захисту кіберсистеми від несанкціонованого доступу полягає в «неможливості» відрізнити деструктивність від «конструктивності» або валідного користувача. Проте існують методики, технології, програмні засоби і системи, здатні ефективно вирішувати питання захисту корпоративного або персонального кіберпростору з наперед заданою вірогідністю проникнення. Існуючі публікації по даному напрямку оперують такими термінами.

Тест проникнень – сукупність зовнішніх і внутрішніх деструктивних впливів, спрямованих на виявлення вразливостей доступу до сервісів КС шляхом моделювання або аналізу проникнень на моделі кіберсистеми.

Якість тесту визначається його повнотою, вираженою у відсотках, щодо перевірки всіх можливих типів вразливостей, що генеруються вручну або автоматично для кожної конкретної кіберсистеми.

Результат тестування реальної системи (System Under Penetration Test - SUPT) формує кількісну оцінку вразливості, а також список структурних вразливостей наперед заданих типів, виявлених в процесі тестового експерименту.

Якщо процес тестування зафіксував непорожній список деструктивних вразливостей, то необхідно виконувати діагностування на основі використання тестів з метою визначення місця, причини і виду вразливості з наперед заданою глибиною пошуку деструктивності.

Після точного визначення всіх вразливостей виконуються процедури їх усунення шляхом часткової або повної реконструкції кіберсистеми на основі використання перевірених бібліотечних структурних рішень.

Всі процедури, згадані вище, використовують три бібліотеки: 1) негативну, що описує всі можливі типи вразливостей; 2) позитивну, де кожній вразливості ставиться у відповідність вірне програмно-апаратне рішення, що усуває деструктивність; 3) неперевірені рішення, складові потенціал «інтелекту» КС, який визначається в процесі експлуатації кіберсистеми. Всі три бібліотеки необхідно поповнювати як в процесі проектування КС, так і на стадії експлуатації в реальному часі.

Завдання інфраструктури захисного сервісу кіберсистеми:

1) Синтез (дедуктивної) моделі КС для тестування, діагностування та відновлення невразливості кіберсистеми.

2) Генерування тестів перевірки та діагностування вразливостей, близьких до 100% повноти.

3) Створення алгоритмів пошуку вразливостей з наперед заданою глибиною діагностування.

4) Створення генераторів тестів перевірки та діагностування вразливостей, близьких до 100% повноті.

5) Тестопридатності проектування (модифікації) невразливих кіберсистем, «вільних» від вразливостей на поточний момент розвитку технологічної та математичної культури.

6) Розробка вбудованої інфраструктури захисного сервісу для кіберсистем, орієнтованих на моніторинг, тестування, діагностування та відновлення невразливості в реальному масштабі часу в процесі експлуатації.

7) Розробка спеціалізованих маршрутів (алгоритмів, планів) моніторингу, тестування, діагностування та відновлення невразливості КС в реальному масштабі часу в процесі експлуатації.
8) Верифікація інфраструктурних тестопридатних рішень, розроблених для реальних КС.
Об'єкт тестування – кібернетична система взаємодіючих програмно-апаратних, телекомунікаційних, інформаційних компонентів, орієнтована на надання якісних сервісів через стандартні інтерфейси санкціонованому користувачеві в реальному масштабі часу. Всі типи вразливостей (проникнень) не виводять об'єкт тестування за кордон заданої функціональності кіберсистеми, представленої булевою функцією:

$$Y = f(X_1, X_2, ..., X_i, ..., X_n),\ X_i, Y \in \{0,1\}.$$

Тому модель вразливостей накладається на графову структуру функціональних модулів, що мають вхідні і вихідні транзакційні змінні. Транзакційний граф представлений дугами – функціональностями (сервісами) з моніторами (ассерція), а також вершинами, що формують стан кіберсистеми за допомогою змінних, пам'яті, інтерфейсних портів введення-виведення інформації, приймачів, терміналів, комп'ютерів: F = (A * B)xS, де S = {S1, S2, ..., Si, ..., Sm} – вершини або стани КС при моделюванні тестових сегментів. Кожен стан Si = {Si1, Si2, ..., Sij, ..., Sip} визначається значеннями істотних змінних КС (змінні, пам'ять, термінали, комп'ютери). Орієнтовані дуги графа є функціональні блоки:

$$B = (B_1, B_2, ..., B_i, ..., B_n),\ \bigcup_{i=1}^{n} B_i = B;\ \bigcap_{i=1}^{n} B_i = \varnothing,$$

де кожному з них може бути поставлена у відповідність ассерція Ai∈A = {A1, A2, ..., Ai, ..., An} для моніторингу функціональностей в часі і в просторі. Існують базові технології тестування безпеки кіберсистем: OSSTMM – The Open Source Security Methodology Manual; NIST Guideline on Network Security Testing; ISACA Switzerland – Testing IT Systems Security With Tiger Teams; Draft Guideline on Network Security Testing; NIST Special Publication 800-26 Security Self-Assessment Guide for Information Technology Systems; Cybersecurity Vulnerability Assessment Methodologies (Cybersecurity VAMs); Information Systems Security Assessment Framework, OISSG.
Функція мети представлена підвищенням ефективності сервісного обслуговування на основі стандартів тестування, граничного сканування і спеціальних технологій діагностування та відновлення невразливості КС, яка визначається мінімальним значенням рівня вразливості, часу відновлення працездатності T і нефункціональної програмно-апаратної надмірності H:

$$E = F(L, T, H) = \min[\frac{1}{3}(L + T + H)],$$

$$Y = (1 - P)^n;$$

$$L = 1 - Y^{(1-k)} = 1 - (1 - P)^{n(1-k)};$$

$$T = \frac{(1 - k) \times H^s}{H^s + H^a};\ H = \frac{H^a}{H^s + H^a},$$

де L – доповнення до рівня невразливості Y, яке залежить від тестопридатності КС k, ймовірності P існування вразливостей і числа невиявлених деструктивних n. Час тестування і діагностування залежить від тестопридатності архітектури k, помноженої на число структурних компонентів інфраструктури, віднесені до загальної кількості елементів КС. Надмірність залежить від структурної складності тестопридатності надбудови, поділеної на програмно-апаратну складність КС. Надмірність інфраструктури забезпечує задану глибину діагностування вразливостей за час, що визначається замовником.

4. Математичний апарат інфраструктури захисного сервісу

Розглянемо метрику, алгебру, структури даних і моделі оцінювання якості взаємодії процесів, явищ, об'єктів і компонентів в кіберпросторі і кіберсистеми, необхідні при створенні ефективних двигунів для обчислювальних процедур аналізу даних в процесах тестування проникнень і відновлення невразливості.
Критерії взаємодії об'єктів тестування грунтуються на використанні бета-метрики вимірювання відстаней в кіберпросторі. Кіберпростір – дискретний векторно-логічний простір – сукупність взаємодіючих за відповідною метрикою інформаційних процесів і явищ, що описуються векторами логічних змінних і використовують як носій комп'ютерні системи та мережі. Метрика – спосіб вимірювання відстані в просторі між компонентами процесів або явищ, описаних векторами логічних змінних. Відстань (булева похідна, ступінь зміни, відмінності або близькості) в кіберпросторі визначається xor-ставленням векторів (матриць), які позначають компоненти процесу або явища, що відрізняє його від кодової відстані по Хеммінгу. Процедури порівняння, вимірювання, оцінювання, розпізнавання, тестування, діагностування оперують xor-ставленням об'єктів або їх компонентів. Компонент простору представлений k-мірним вектором a = {a1, a2, ..., aj,

..., ak}, ai ∈{0,1}, де кожна його координата визначена в двійковому алфавіті, 0 – «неправда», 1 – «істина» . Нуль-вектор є k-мірний кортеж, всі координати якого дорівнюють нулю: aj = 0, j = 1, ..., k.

Метрика β кібернетичного простору визначається рівністю, яке формує нуль-вектор для xor-суми відстаней di між ненульовим і кінцевим числом об'єктів, замкнутих в цикл. Тут n – кількість відстаней між компонентами (векторами) простору, складовими циклу D = {d1, d2, ..., di, ..., dn}, di – є вектор відстані, відповідний ребру циклу, що з'єднує два компонента (вектора) a, b простору, який далі позначається без індексу як d (a, b). Відстань між двома об'єктами a і b є похідний вектор $d(a,b) = (aj \oplus bj)_1^k$. Векторному значенню відстані відповідає норма (скаляр), що визначається кодовою відстанню по Хеммінгу між двома векторами у вигляді числа одиниць вектора d (a, b). Метрика β векторного логічного двійкового простору є рівна нуль-вектору xor-сума відстаней між кінцевим числом вершин графа, що утворюють цикл. Тепер можна дати більш формальне визначення кіберпростору, як векторно-логічного, нормованого бета-метрикою, де xor-сума відстаней між кінцевим числом точок циклу дорівнює нуль-вектору. Визначення метрики через відносини дозволяє скоротити систему аксіом (рефлексивності, сімметрчності і транзитивності, трикутного замикання) з трьох до одного і поширити її дію на як завгодно складні структури n-мірного логічного простору. Класичне завдання метрики для визначення взаємодії однієї, двох і трьох точок у векторному логічному просторі є окремим випадком бета-метрики при i = 1,2,3 відповідно. Визначення метрики через відносини дозволяє скоротити систему аксіом (рефлексивності, сімметрчності і транзитивності, трикутного замикання) з трьох до одного і поширити її дію на як завгодно складні структури n-мірного логічного простору. Класичне завдання метрики для визначення взаємодії однієї, двох і трьох точок у векторному логічному просторі є окремим випадком бета-метрики при i = 1,2,3 відповідно $\beta = \bigoplus_{i=1}^{n} d_i = 0$:

$$M \subset \beta = \begin{cases} d_1 = 0 \leftrightarrow a = b; \\ d_1 \oplus d_2 = 0 \leftrightarrow d(a,b) = d(b,a); \\ d_1 \oplus d_2 \oplus d_3 = 0 \leftrightarrow d(a,b) \oplus d(b,c) = d(a,c). \end{cases}$$

Векторно-логічний транзитивний трикутник має повну аналогію з чисельним виміром відстані в метричному M-просторі, який задається системою аксіом, що визначає взаємодію однієї, двох і трьох точок в будь-якому просторі:

$$M = \begin{cases} d(a,b) = 0 \leftrightarrow a = b; \\ d(a,b) = d(b,a); \\ d(a,b) + d(b,c) \geq d(a,c). \end{cases}$$

Специфіка аксіоми трикутника (метричного) M-простору полягає в чисельному (скалярному) порівнянні відстаней трьох об'єктів. При цьому інтервальна невизначеність відповіді – дві сторони трикутника можуть бути більші або рівні третій – малопридатна для визначення точної довжини останньої сторони. Бета-метрика усуває даний недолік і виключає невизначеність бінарного відношення детермінованих процесів або явищ. Третя сторона трикутника у векторному логічному просторі визначається двійковим вектором-відстанню між двома вершинами шляхом обчислення xor-суми відстаней двох інших сторін трикутника:

$$d(a,b) \oplus d(b,c) = d(a,c) \rightarrow d(a,b) \oplus d(b,c) \oplus d(a,c) = 0.$$

Метрика β кібернетичного багатозначного векторно-логічного простору є вектор, що дорівнює значенню Ø по всіх координатах, отриманий шляхом застосування симетричної різниці відстаней між кінцевим числом точок, що утворюють цикл:

$$\beta = \Delta_{i=1}^{n} d_i = \varnothing.$$

Тут кожна координата вектора, відповідного об'єкту, визначена в алфавіті, що становить булеан на універсумі примітивів потужністю p:

$$a_j = \{\alpha_1, \alpha_2, ..., \alpha_r, ..., \alpha_m\}, m = 2^p.$$

На основі введеної метрики аналізу кіберпростору вводяться критерії оцінювання взаємодії кінцевого числа об'єктів між собою. Скалярний критерій взаємодії двох об'єктів (процесів) в дискретному булевому просторі, представлених k-мірними багатозначними векторами

$$m = (m_1, m_2, ..., m_j, ..., m_k),\ m_j \in \{0,1,x\};$$
$$A = (A_1, A_2, ..., A_j, ..., A_k),\ A_j \in \{0,1,x\},$$

необхідний для порівняння і подальшого вибору, кращого в деякому сенсі, рішення. Ступінь належності m-вектора до A-вектора $\mu(m \in A)$ позначається як неналежність $\bar{\mu}(m \in A)$. Існує 5 типів теоретико-множинної взаємодії двох векторів:

$$1)\ m = A;\ 2)\ m \subset A;\ 3)\ A \subset m;\ 4)\ m \cap A \neq \{m, A, \varnothing\};\ 5)\ m \cap A = \varnothing.$$

Мета скалярного критерію – оцінити будь-яке з зазначених взаємодій інтервальною оцінкою [0,1] шляхом спільного використання трьох параметрів: кодової відстані d (m, A) і двох функцій неналежності

$$\bar{\mu}(m \in A) = 1 - \mu(m \in A),\ \bar{\mu}(A \in m) = 1 - \mu(A \in m).$$

$$Q = \frac{1}{3}\left[\frac{1}{k}d(m,A) + [1-\mu(m \in A)] + [1-\mu(A \in m)]\right],$$

$$d(m,A) = \mathrm{card}\,(m_i \underset{i=1}{\overset{k}{\cap}} A_i = \varnothing);$$

$$\mu(m \in A) = 2^{c-a};$$

$$\mu(A \in m) = 2^{c-b};$$

$$a = \mathrm{card}\,(A_i = x), i = \overline{1,k};$$

$$b = \mathrm{card}\,(m_i = x), i = \overline{1,k};$$

$$c = \mathrm{card}\,(m_i \underset{i=1}{\overset{k}{\cap}} A_i = x).$$

Тут

$$d(m,A) = \mathrm{card}\,(m_i \underset{i=1}{\overset{k}{\cap}} A_i = \varnothing)$$

– потужність або кількість порожніх координатних перетинів двох взаємодіючих векторів, що складають відстань по Хеммінгу;

$$\mu(m \in A) = 2^{c-a} \ (\mu(A \in m) = 2^{c-b})$$

– відношення загального для m і A простору до простору вектора A (m), що формує зазначену функцію належності. Операції координатного перетину (and), симетричної різниці (xor) визначені для символів алфавіту Кантора A = {0,1, x = {0,1}, Ø}, кодованих векторами (01,10,11,00) відповідно:

∩	0	1	x	∅
0	0	∅	0	∅
1	∅	1	1	∅
x	0	1	x	∅
∅	∅	∅	∅	∅

∧	01	10	11	00
01	01	00	01	00
10	00	10	10	00
11	01	10	11	00
00	00	00	00	00

Δ	0	1	x	∅
0	∅	x	1	0
1	x	∅	0	1
x	1	0	∅	x
∅	0	1	x	∅

⊕	0	1	x	∅
0	00	11	10	01
1	11	00	01	10
x	10	01	00	11
∅	01	10	11	00

Нормування параметрів критерію (кодової відстані і функцій неналежності) дозволяє оцінити рівень взаємодії векторів в чисельному інтервалі [0,1]. З урахуванням ізоморфізму теоретико-множинних і логічних операцій критерій якості можна трансформувати до виду:

$$Q = \frac{1}{3}\left[\frac{1}{k}d(m,A) + [1-\mu(m \in A)] + [1-\mu(A \in m)]\right],$$

$$d(m,A) = \mathrm{card}\,(m_i \underset{i=1}{\overset{k}{\oplus}} A_i = U);$$

$$\mu(m \in A) = \mathrm{card}\,(A_i = U) - \mathrm{card}\,(m_i \underset{i=1}{\overset{k}{\wedge}} A_i = U);$$

$$\mu(A \in m) = \mathrm{card}\,(m_i = U) - \mathrm{card}\,(m_i \underset{i=1}{\overset{k}{\wedge}} A_i = U);$$

$$U = \begin{cases} 1 \leftarrow \{m_i, A_i\} \in \{0,1\}; \\ x \leftarrow \{m_i, A_i\} \in \{0,1,x\}. \end{cases}$$

Якщо вектори m і A – виконавчі по всіх координатах, то змінна U = 1 і обчислення проводяться за правилами двійкової операції. Якщо вектори m і A визначені в троїчному алфавіті, то змінна U = x ініціює обчислення на основі використання теоретико-множинної операції симетричної різниці. Перший компонент d (m, A) / n критерію формує ступінь розбіжності k-мірних векторів у вигляді кодової відстані по Хеммінгу, віднесеної до довжини вектора, шляхом виконання операції xor над усіма координатами; другий і третій компоненти

$$[1-\mu(m \in A)] + [1-\mu(A \in m)]$$

визначають ступень неналежності результату кон'юнкції до простору кожного з двох взаємодіючих векторів. Якщо такі міри дорівнюють нулю

$$\frac{1}{n}d(m,A) = 0, [1-\mu(m \in A)] = 0, \ [1-\mu(A \in m)] = 0,$$

то об'єкти ідентичні один одному. Поняття власності і неналежність є взаємодоповнюючими, але в даному випадку більш технологічно обчислювати неналежність, оскільки загальноприйнятим в літературі є поняття нульової розбіжності об'єктів, що свідчить про їх повну ідентичність. Цей критерій працює в інтервалі [0,1]. Повний збіг двох об'єктів

$$d(m,A) = 0, \ \mu(m \in A) = 1, \ \mu(A \in m) = 1$$

характеризується нульовою оцінкою критерію

$$Q = \frac{1}{3}\left[\frac{1}{k}0 + [1-1] + [1-1]\right] = 0.$$

Протилежним варіантом оцінювання є максимальна розбіжність двох об'єктів:

$$d(m,A) = k, \ \mu(m \in A) = 0, \ \mu(A \in m) = 0,$$

яка визначається оцінкою взаємодії:

$$Q = \frac{1}{3}\left[\frac{1}{k}k + [1-0] + [1-0]\right] = 1.$$

Якщо параметри взаємодії рівні

$$d(m,A) = 0, \ \mu(m \in A) = \frac{1}{2}, \ \mu(A \in m) = \frac{1}{2},$$

то критерій буде мати таку оцінку:

$$Q = \frac{1}{3}\left[\frac{1}{k}0 + [1-\frac{1}{2}] + [1-\frac{1}{2}]\right] = \frac{1}{3}.$$

Взаємодія (перетин) двох векторів: A = (XXX1X) і m = (XX0X0) дає загальний простір, рівний (XX010) = {00010, 01010, 10010, 11010}. Критерій якості взаємодії при параметрах

$$d(m, A) = 0,\ \mu(m \in A) = \frac{1}{2},\ \mu(A \in m) = \frac{1}{4}$$

матиме таку оцінку:

$$Q = \frac{1}{3}\left[\frac{1}{k}0 + [1-\frac{1}{2}] + [1-\frac{1}{4}]\right] = \frac{1}{4}.$$

Перевага введеного критерію (неналежність, відмінності) полягає в лінійності зміни його чисельного значення від 0 до 1 в міру збільшення «відстані» від повного збігу двох об'єктів до максимально можливого, коли кодова відстань одно d(m, A)=k.

Критерій може бути використаний в задачах відстеження цілі, руху по заданому маршруту, тестування і діагностування функціональних порушень і вразливостей, пошуку, розпізнавання та прийняття рішень. Критерій якості Q, застосовуваний для виконання регуляторної функції при оцінюванні взаємодії об'єктів в реальному масштабі часу, необхідно мінімізувати.

Проте скалярна оцінка має лише інтегральні властивості взаємодії двох об'єктів, що дозволяє здійснювати порівняння декількох відстаней, частіше міри близькості одного об'єкта по відношенню до кінцевої множини інших. Недоліком інтегральної оцінки є неоднозначність її приведення до початкового векторного еквіваленту, як і будь-якого іншого функціонального відношення: пряма імплікація однозначна, зворотна – багатозначна. Тому повна картина аналізу взаємодії об'єктів повинна містити не тільки інтегральний скалярний критерій Q, але і результат їх векторного відношення Q (m, A) = m⊕A, який більш інформативний для подальшої корекції напрямку вирішення завдань синтезу або аналізу процесів взаємодії в рамках існуючої системи. Як отримати векторний критерій якості взаємодії двох об'єктів? Формула скалярного критерію якості після проведення векторних операцій використовує процедури обчислення трьох компонентів: кодова відстань, яке визначається числом одиниць в координатах результуючого вектора, отриманого на основі xor-операції, d (m, A) = m⊕A і дві функції приналежності:

$$\mu = \mu(m \in A) \vee \mu(A \in m) = (A \wedge \overline{m \wedge A}) \vee (m \wedge \overline{m \wedge A}),$$

які в сукупності також визначаються xor-операцією, в загальному випадку на замкнутому теоретико-множинному алфавіті:

$$\mu = (A \wedge \overline{m \wedge A}) \vee (m \wedge \overline{m \wedge A}) = [A \wedge (\overline{m} \vee \overline{A})] \vee [m \wedge (\overline{m} \vee \overline{A})] =$$
$$= [(A \wedge \overline{m}) \vee (A \wedge \overline{A}) \vee (m \wedge \overline{m}) \vee (m \wedge \overline{A})] =$$
$$= (A \wedge \overline{m}) \vee (m \wedge \overline{A}) = m \oplus A.$$

Логічне об'єднання двох векторних функцій, які формують кодову відстань і взаємну належність один одному, дає, природно, шуканий результат:

$$Q = d(m, A) \vee [\mu(m \in A) \vee \mu(A \in m)] =$$
$$= (m \oplus A) \vee (m \oplus A) = m \oplus A.$$

Це означає, що по суті взаємодія будь-яких об'єктів в кіберпросторі визначається виконанням симетричної різниці в багатозначному алфавіті (xor-операції в двійковому):

Δ	0	1	x	∅
0	∅	x	1	0
1	x	∅	0	1
x	1	0	∅	x
∅	0	1	x	∅

0=01; 1=10
x=11; ∅=00 →

⊕	0	1	x	∅
0	00	11	10	01
1	11	00	01	10
x	10	01	00	11
∅	01	10	11	00

Але при кодуванні символів алфавіту двійковими векторами-примітивами операція симетричної різниці між символами в координатах векторів перетворюється в xor-операцію довічних векторів. Інші логічні операції при формуванні векторної оцінки взаємодії об'єктів в кіберпросторі, згідно з наведеними вище формулами, не використовуються. Як приклад, нижче запропоновані процедури виконання операції симетричної різниці і xor над двома формами об'єктів, представленими у вигляді символів алфавіту Кантора і двійкових кодів:

m =	x	x	x	x	1	0	1	0
A =	1	0	0	x	x	x	1	0
Δ =	0	1	1	∅	0	1	∅	∅
m =	11	11	11	11	10	01	10	01
A =	10	01	01	11	11	11	10	01
⊕ =	01	10	10	00	01	10	00	00

Другий приклад ілюструє обчислення взаємодії векторів в двотактному алфавіті опису автоматних змінних B2 (Y) в форматах символьного і довічного опису координат:

m =	Y	A	B	S	P	L	E	Q
A =	H	S	J	L	E	L	F	C
Δ =	L	B	H	E	H	∅	Y	Y
m =	1111	1100	0011	1001	0110	1101	0100	1000
A =	0010	1001	0001	1101	0100	1101	1011	0111
⊕ =	1101	0101	0010	0100	0010	0000	1111	1111

Тут цікавий факт, що в кубітному форматі опису символьних змінних теоретико-множинні, в загальному випадку послідовно виконувані, операції над елементами множин замінюються паралельними операціями, що істотно підвищує швидкодію обчи-

слювальних процесів аналізу моделей за рахунок відповідного збільшення обсягу пам'яті. Для створення кубітних структур даних обчислювальних процесів необхідно визначити: 1) універсум примітивів (процесів або явищ) з подальшим їх унітарним кодуванням в межах кубіта; 2) компактну систему (структуру) відносин (функціональних), які задають поведінку об'єкта; 3) послідовність обробки компонентів структури на основі паралельного виконання векторних логічних операцій, які вигідно відрізняють теоретико-множинні, послідовні в часі, обчислювальні процедури.

Дві форми (скалярна і векторна) існування критерію якості q = {Q, Q (m, A)} спрямовані на вибір кращого рішення (для користувача) і деталізацію відмінностей між об'єктами (для комп'ютера) відповідно. Чисельний еквівалент зручний для людини, яка не здатна оперувати лінгвістичними (багатозначними) змінними при оцінці взаємодії об'єктів, представлених векторами. До того ж дві однакові чисельні оцінки не означають ідентичності двох відстаней при взаємодії трьох об'єктів у просторі. Наприклад: d (a, b) = 0011 = 2, d (a, c) = 1100 = 2, при a = 0000 b = 1100, c = 0011. Тому до скалярної оцінки необхідно мати векторний еквівалент критерію якості взаємодії, який показує структуру подібності та відмінності за всіма параметрами (змінним) векторів.

Обчислити критерій – визначити ступінь належності чи неналежності даного процесу або явища, в тому числі до деякого класу об'єктів. Така класифікація шляхом порівняння аналізованого об'єкта з сімейством, але представленим у формі одного узагальненого вектора, дає можливість істотно підвищити швидкодію завдань аналізу структур даних. Для цього необхідно створювати ієрархічні формати структур даних, орієнтованих на компактне уявлення спеціальним чином закодованих об'єктів. При поданні об'єкта кіберпростору сукупністю теоретико-множинних або кубітних змінних структура вектора ділиться на сегменти, відповідні кубітам. Кубітна змінна (кубіт) – сукупність n двійкових розрядів, необхідних для унітарної кодування n примітивів і булеана породжених символів. Форми подання вектора кубітних змінних: символьна і / або кубітно-двійкова орієнтовані на паралельне виконання теоретико-множинних операцій $(\cap,\cup,\tilde{m})$ за допомогою алгебри векторної логіки $(\wedge,\vee,\overline{m})$. Приклади таких операцій в згаданих форматах мають вигляд:

m =	Y	A	B	S	P	L	E	Q
A =	H	S	J	L	E	L	F	C
∩ =	H	Q	J	S	E	L	∅	∅
m =	1111	1100	0011	1001	0110	1101	0100	1000
A =	0010	1001	0001	1101	0100	1101	1011	0111
∨ =	0010	1000	0001	1001	0100	1101	0000	0000
m =	Y	A	B	S	P	L	E	Q
$\tilde{m}$ =	∅	B	A	P	S	H	F	C
m =	1111	1100	0011	1001	0110	1101	0100	1000
$\overline{m}$ =	0000	0011	1100	0110	1001	0010	1011	0111

При аналізі кубітно-двійкових форм представлення об'єктів в цілях визначення відстаней між ними необхідно враховувати: 1) Кодова відстань формується при наявності хоча б одного кубіта, рівного нулю по всіх його координатах. 2) В іншому випадку обчислюються функції належності на підставі підрахунку загального числа одиниць, отриманого при виконанні векторної операції кон'юнкції, віднесених до кількості одиниць кожного з векторів, що відповідають двом різним об'єктам кіберпростору. 3) Xor-сума відстаней об'єктів, що становлять цикл, дорівнює вектору, складеному з нульових кубітів. 4) Xor-сума всіх примітивів кубіта дорівнює вектору, який має всі одиничні координати. 5) Формування багатозначних сигнатур на основі кубітних структур даних може істотно розширити сферу застосування апарату xor-поліномів з нелінійними зворотними зв'язками. 6) Неструктурована множина примітивів, що самоорганізується в процесі моделювання або вирішення конкретного завдання, істотно зменшує обсяг моделей і час їх створення. 7) Реалізація дерева класифікації і процедур його аналізу значно скорочує обсяг структур даних, а також час вирішення відповідних завдань. Приклад такого дерева представлений на рис. 6, яке, завдяки бінарної, виконує класифікацію (спуск по дереву) за мінімальне число кроків обчислювальної процедури.

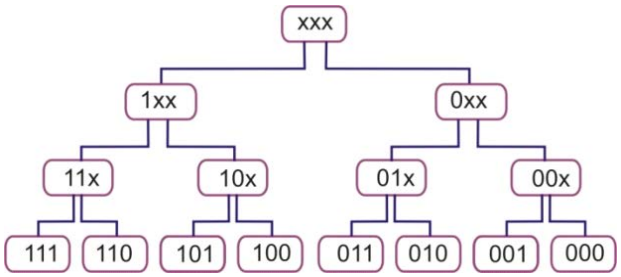

Рис. 6. Приклад класифікаційного бінарного дерева

Процедура класифікації: 1) Аналіз і-го розряду вхідного вектора m для вибору лівої чи правої гілки вершини дерева:

$$P = \begin{cases} P^0 \leftarrow m_i \oplus A_i = 0; \\ P^1 \leftarrow m_i \oplus A_i = 1. \end{cases}$$

Тут множина А визначає узагальнені коди-сигнатури, а також кінцеві вершини дерева. 2) Аналіз закінчується позитивно, якщо оброблені всі розряди вхідного вектора, який ідентифікований існуючим аналогом в бібліотеці. В іншому випадку об'єкт не може бути ідентифікований в рамках системи, яка повинна бути розширена. 3) Якщо результат аналізу має неоднозначність по відношенню до 0 і 1, то об'єкт ідентифікується вже не примітивом, а класом (підкласом). Час виконання процедури класифікації визначається виразом: T = log2N, що є заслугою надлишкових вершин, які дозволяють систему з N відносин (нижній рівень кодів) представити у вигляді дерева.

Таким чином, запропонована модифікована модель критерію скалярної і векторної якості оцінювання бінарних відносин, яка відрізняється використанням функції неналежності та кодової відстані Хеммінга, що забезпечує лінійність зміни чисельного значення критерію від 0 до 1 в міру збільшення «відстані» від повного збігу двох об'єктів до максимально можливого , коли кодова відстань одно d (m, A) = k. Критерій може бути використаний при оцінюванні взаємодії об'єктів в реальному масштабі часу в задачах тестування, діагностування функціональних порушень, вразливостей.

5. Апарат булевих похідних для синтезу тестів

Апарат призначений для перевірки суттєвості змінних і компонентів КС, включаючи аналіз суттєвості деструктивності (уразливості і проникнення) для стану кіберсистеми. Розглядаються методи взяття булевих похідних по таблиці істинності, диз'юнктивній формі або кубічному покриттю для створення умов активізації на вхідних змінних при синтезі тестів для перевірки вразливостей (проникнень). Дослідження методу пропонується виконати за допомогою трьох прикладів логічних функцій:

$$1)\ f(x) = x_1 \vee x_1\bar{x}_2;\ 2)\ f(x) = x_1x_2 \vee \bar{x}_1x_3\ ;$$
$$3)\ f(x) = \bar{x}_2\bar{x}_3 \vee x_1x_2x_3.$$

Питання, що підлягають вирішенню: 1) Визначення всіх похідних першого порядку по аналітичній, кубічній і табличній формі завдання логічної функції. 2) Верифікація отриманих умов активізації шляхом їх моделювання на одній з форм опису функціональності. 3) Синтез тестів активізації змінних логічної функції на основі обчислення похідних.

Приклад 1. Визначити всі похідні першого порядку по аналітичній формі логічної функції $f(x) = x_1 \vee x_1\bar{x}_2$. Застосування формули обчислення

$$f'(x_i) = df(x_1, x_2, \ldots, x_i, \ldots, x_n)/dx_i =$$
$$= f(x_1, x_2, \ldots, x_i=0, \ldots, x_n) \oplus f(x_1, x_2, \ldots, x_i=1, \ldots, x_n)$$

визначає булеву похідну першого порядку як суму по модулю для нульової і одиничної залишкових функцій.

Для даної функції виходить:

$$\frac{df(x_1, x_2)}{dx_1} = f(0, x_2) \oplus f(1, x_2) =$$
$$= (0 \vee 0\bar{x}_2) \oplus (1 \vee 1\bar{x}_2) = 0 \oplus 1 = 1;$$
$$\frac{df(x_1, x_2)}{dx_2} = f(x_1, 0) \oplus f(x_1, 1) =$$
$$= (x_1 \vee x_1 \cdot 1) \oplus (x_1 \vee x_1 \cdot 0) = x_1 \oplus x_1 = 0.$$

Нульове значення похідної означає відсутність умов активізації змінної x2, що дає підстави вважати її несуттєвою, а отже, прибрати з числа змінних, які формують функціональність.

Приклад 2. Визначити всі похідні першого порядку по аналітичній формі логічної функції $f(x) = x_1x_2 \vee \bar{x}_1x_3$. Для даної функції виконуються такі обчислення:

$$\frac{df(x_1, x_2, x_3)}{dx_1} = f(0, x_2, x_3) \oplus f(1, x_2, x_3) =$$
$$= (0 \vee 1 \cdot x3) \oplus (x2 \vee 0 \cdot x3) = x3 \oplus x2 = x_2\overline{x_3} \vee \overline{x_2}x_3;$$
$$\frac{df(x_1, x_2, x_3)}{dx_2} = f(x_1, 0, x_3) \oplus f(x_1, 1, x_3) = \bar{x}_1x_3 \oplus (x_1 \vee x_3) =$$
$$\overline{\bar{x}_1x_3}(x_1 \vee x_3) \vee \bar{x}_1x_3\overline{(x_1 \vee x_3)} = (x_1 \vee \bar{x}_3)(x_1 \vee x_3) \vee \bar{x}_1x_3\bar{x}_1\bar{x}_3 = x_1.$$
$$\frac{df(x_1, x_2, x_3)}{dx_3} = f(x_1, x_2, 0) \oplus f(x_1, x_2, 1) = x_1x_2 \oplus (\bar{x}_1 \vee x_2) =$$
$$\overline{x_1x_2}(\bar{x}_1 \vee x_2) \vee x_1x_2\overline{(\bar{x}_1 \vee x_2)} = (\bar{x}_1 \vee \bar{x}_2)(\bar{x}_1 \vee x_2) \vee x_1x_2x_1\bar{x}_2 = \bar{x}_1.$$

Для трьох змінних отримані 4 умови активізації, які відповідають чотирьом логічним шляхav в схемній структурі диз'юнктивної форми даної функції.

Приклад 3. Визначити всі похідні першого порядку по кубічній формі логічної функції:

$f(x) = \bar{x}_2\bar{x}_3 \vee x_1x_2x_3 =$

x_1	x_2	x_3	Y
X	0	0	1
1	1	1	1
X	0	1	0
X	1	0	0
0	1	X	0

$=$

x_2x_3 / x_1	00	01	11	10
0	1	0	0	0
1	1	0	1	0

$=$

x_1	x_2	x_3	Y
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Процес-модель обчислення похідної по змінній для функції x_i, заданої табличною формою, має такі пункти: 1) Моделювання по таблиці істинності (кубічному покриттю) вхідних наборів для визначення стовпчика Y_i^0, де змінна x_i має тільки нульове значення для всіх рядків таблиці істинності. Число таких наборів завжди $q=2^{n-1}$, N – число змінних. 2) Обчислення координат стовпчика Y_i^1 з одиничним значенням змінної $Y_i^{\oplus} = Y_i^0 \oplus Y_i^1$ для всіх рядків таб-

лиці. 3) Обчислення стовпчика з урахуванням правила $0 \oplus X \vee 1 \oplus X = X$. 4) Формування диз'юнктивної форми похідної функції за одиничними значеннями стовпчика $Y_i^{\oplus}$ без змінної xi, по якій береться похідна. Інакше, фіксуються рядки таблиці, відповідні одиничним значенням стовпця $Y_i^{\oplus}$, який визначає похідну функції. Аналітична модель процесу взяття похідної по функції, представленої таблицею, має такий вигляд:

$$df/dx_i = f(x_1, x_2, \ldots, x_i=0, \ldots, x_n) \oplus f(x_1, x_2, \ldots, x_i=1, \ldots, x_n);$$

$$Y_i^{\oplus} = [Y_i^0 = f(x_1, x_2, \ldots, x_i=0, \ldots, x_n)] \oplus$$

$$\oplus [Y_i^1 = f(x_1, x_2, \ldots, x_i=1, \ldots, x_n)].$$

Для двох різних табличних форм результат обчислення похідної за першою змінною представлений нижче:

$\frac{df}{dx_1} =$

x_1	x_2	x_3	Y	Y_1^0	Y_1^1	$Y_1^{\oplus}$
X	0	0	1	1	1	0
1	1	1	1	0	1	1
X	0	1	0	0	0	0
X	1	0	0	0	0	0
0	1	X	0	0	X	1

$= x_2 \vee x_2 x_3 = x_2 x_3;$

$\frac{df}{dx_1} =$

x_1	x_2	x_3	Y	Y_1^0	Y_1^1	$Y_1^{\oplus}$
0	0	0	1	1	1	0
0	0	1	0	0	0	0
0	1	0	0	0	0	0
0	1	1	0	0	1	1
1	0	0	1	1	1	0
1	0	1	0	0	0	0
1	1	0	0	0	0	0
1	1	1	1	0	1	1

$= x_2 x_3.$

При неоднозначному значенні похідної для функції, заданої кубічним покриттям, вибирається терм, що має максимальне число змінних. Мінімізація похідної функції на основі тотожності $a \vee ab = a$ не зберігає умови активізації змінної, по якій береться похідна. Справді, значення функції від трьох змінних за умови $a\bar{b} \vee ab$ може дорівнювати нулю (одиниці), що означає можливість відсутності зміни функції при активізації змінної «c» (останній стовпець карти Карно):

ab / c	00	01	11	10
0	1	0	0	0
1	1	0	1	0

Лема неперетинання кубів. Можливість коректного взяття похідної для отримання тесту активізації по змінній x_i обмежується такою мінімальною структурою кубічного покриття або аналітичною диз'юнктивною (кон'юнктівною) нормальною формою, де перетин будь-яких кубів (рядків таблиці істинності) або термів ДНФ (КНФ) дає порожню множину:

$$df/dx_i = f(x_1, x_2, \ldots, x_i=0, \ldots, x_n) \oplus f(x_1, x_2, \ldots, x_i=1, \ldots, x_n) \in T \leftrightarrow \forall i,j (Ci \cap Cj = \varnothing);\ i,j=1,\ldots,n;\ i \neq j.$$

Дійсно, якщо покриття, представлене вище, записати за правилами перетинання кубів, то всі похідні будуть валідними для синтезу тестів без додаткової перевірки:

$f(x) = \bar{x}_2 \bar{x}_3 \vee x_1 x_2 x_3 =$

x_1	x_2	x_3	Y
X	0	0	1
1	1	1	1
X	0	1	0
X	1	0	0
0	1	X	0

$\rightarrow$

x_1	x_2	x_3	Y
X	0	0	1
1	1	1	1
X	0	1	0
X	1	0	0
0	1	1	0

Щоб отримати таке кубічне покриття, необхідно виконувати мінімізацію усіма існуючими методами (карти Карно, Квайна, істотних змінних, невизначених коефіцієнтів, бінарного графа) з урахуванням цього правила: покриття нульових і одиничних координат таблиці істинності в процесі мінімізації не повинні перетинатися. В даному випадку, коли функціональність переписана з урахуванням даного правила, навіть загальне число кубів не змінилося, в той час як покриття набуло якості неперетинання (як у таблиці істинності) для синтезу тестів активізації змінних:

$\frac{df}{dx_1} =$

x_1	x_2	x_3	Y	Y_2^0	Y_2^1	$Y_2^{\oplus}$
X	0	0	1	1	1	0
1	1	1	1	0	1	1
X	0	1	0	0	0	0
X	1	0	0	0	0	0
0	1	1	0	0	0	0

$= x_2 x_3;$

$\frac{df}{dx_1} =$

x_1	x_2	x_3	Y	Y_2^0	Y_2^1	$Y_2^{\oplus}$
0	0	0	1	1	1	0
0	0	1	0	0	0	0
0	1	0	0	0	0	0
0	1	1	0	0	1	1
1	0	0	1	1	1	0
1	0	1	0	0	0	0
1	1	0	0	0	0	0
1	1	1	1	0	1	1

$= x_2 x_3.$

Обчислення похідних по всіх вхідних змінних дає можливість побудувати тест активізації для функціональності, заданої вже не таблицею істинності, а кубічним покриттям, що може істотно зменшити час синтезу тестів. Для другої змінної функції $f(x) = \bar{x}_2 \bar{x}_3 \vee x_1 x_2 x_3$ процес обчислення похідних для трьох різних форм (кубічної, табличної і аналітичної) має наступний вигляд:

$\frac{df}{dx_2} =$

x_1	x_2	x_3	Y	Y_2^0	Y_2^1	$Y_2^{\oplus}$
X	0	0	1	1	0	1
1	1	1	1	0	1	1
X	0	1	0	0	X	X
X	1	0	0	1	0	1
0	1	1	0	0	0	0

$= \bar{x}_3 \vee x_1 x_3 \vee \bar{x}_3 = \bar{x}_3 \vee x_1 x_3;$

x_1	x_2	x_3	Y	Y_2^0	Y_2^1	$Y_2^{\oplus}$
0	0	0	1	1	0	1
0	0	1	0	0	0	0
0	1	0	0	1	0	1
0	1	1	0	0	0	0
1	0	0	1	1	0	1
1	0	1	0	0	1	1
1	1	0	0	1	0	1
1	1	1	1	0	1	1

$= \vee \bar{x}_1 \bar{x}_3 \vee x_1 \bar{x}_3 \vee x_1 x_3 = \bar{x}_3 \vee x_1 x_3;$

Аналогічний результат отриманий шляхом визначення похідної за диз'юнктивною нормальною формою логічної функції:

$df(x_1,x_2,x_3)/dx_2 = f(x_1,0,x_3) \oplus f(x_1,1,x_3) = x_1x_3 \vee \bar{x}_3$.

Для третьої змінної функції $f(x) = \bar{x}_2\bar{x}_3 \vee x_1x_2x_3$ похідні від трьох різних форм (кубічної, табличної і аналітичної) представлені у такому вигляді:

$$\frac{df}{dx_3} =$$

x_1	x_2	x_3	Y	Y_3^0	Y_3^1	$Y_3^{\oplus}$
X	0	0	1	1	0	1
1	1	1	1	0	1	1
X	0	1	0	0	0	0
X	1	0	0	0	X	X
0	1	1	0	0	0	0

$= \bar{x}_2 \vee x_1x_2;$

x_1	x_2	x_3	Y	Y_3^0	Y_3^1	$Y_3^{\oplus}$
0	0	0	1	1	0	1
0	0	1	0	1	0	1
0	1	0	0	0	0	0
0	1	1	0	0	0	0
1	0	0	1	1	0	1
1	0	1	0	1	0	1
1	1	0	0	0	1	1
1	1	1	1	0	1	1

$= \vee \bar{x}_1\bar{x}_2 \vee x_1\bar{x}_2 \vee x_1x_2 = \bar{x}_2 \vee x_1x_2.$

$df(x_1,x_2,x_3)/dx_3 = f(x_1,x_2,0) \oplus f(x_1,x_2,1) = x_1x_2 \vee \bar{x}_2$.

Таким чином, всі результати по обчисленню похідних від трьох форм завдання функції ідентичні. Найбільш технологічним є метод взяття похідної по таблиці істинності. Але використання кубічного покриття має меншу обчислювальну складність в силу компактного представлення функціональності за рахунок введення надмірності (символу X) в двійковий алфавіт. Використання аналітичної форми передбачає істотне підвищення складності алгоритмів, пов'язаної із застосуванням законів булевої алгебри і мінімізації функцій, що обмежує її застосування для вирішення практичних завдань.

Процес-модель отримання тесту

$$T = [T_{ij}],\ i = \overline{1,k};\ j = \overline{1,n}$$

комбінаційної функціональності:

1) $f'(x_i) = f(x_1, x_2, \ldots, x_i = 0, \ldots, x_n) \oplus f(x_1, x_{2,\ldots,} x_i = 1, \ldots, x_n)$;

2) $T = \bigcup_{i=1}^{n} [f'(x_i) * (x_i = 0) \vee (x_i = 1)]$;

3) $T_{ij} = T_{i-1,j} \leftarrow T_{ij} = X;\ T_{1j} = 1 \leftarrow T_{1j} = X$;

4) $T = T \setminus T_i \leftarrow T_i = T_{i-r},\ r = \overline{1, i-1},\ i = \overline{2,n}$.

1) Обчислення похідних по всіх n змінних функціональності шляхом використання однієї з форм: аналітичної, табличної, кубічної. 2) Об'єднання всіх умов (векторів) активізації в таблицю, де кожному вектору шляхом конкатенації (*) ставиться у відповідність зміна адреси, за якою була взята похідна, що означає подвоєння числа тестових наборів по відношенню до загальної кількості (k) умов активізації. 3) Довизначення символу X = {0,1} в координаті шляхом присвоєння довічного значення однойменної координати в попередньому векторі для отримання тесту мінімальної довжини. 4) Мінімізація тестових векторів шляхом видалення повторюваних вхідних послідовностей.

Рис. 7 ілюструє таблиці ходу отримання тесту відповідно до пунктів 2-4 алгоритму для функціональності $f(x) = \bar{x}_2\bar{x}_3 \vee x_1x_2x_3$, представленої схемною структурою.

$$T =$$

x_1	x_2	x_3	Y
0	1	1	0
1	1	1	1
X	0	0	1
X	1	0	0
1	0	1	0
1	1	1	1
X	0	0	1
X	0	1	0
1	1	0	0
1	1	1	1

$=$

x_1	x_2	x_3	Y
0	1	1	0
1	1	1	1
1	0	0	1
1	1	0	0
1	0	1	0
1	1	1	1
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

$=$

x_1	x_2	x_3	Y
0	1	1	0
1	1	1	1
1	0	0	1
1	1	0	0
1	0	1	0

Рис. 7. Таблиці тестів і схемна структура булевої функції

Отриманий тест за кількістю і якістю ідентичний вхідним наборам, синтезованим раніше за допомогою F⊕L-методу. Отже, він має однакові властивості по покриттю несправностей і глибині пошуку дефектів.

Запропонована процес-модель синтезу тестів для тестування і діагностування вразливостей може бути використана як вбудований компонент інфраструктури сервісного обслуговування КС.

6. Дедуктивний метод пошуку вразливостей в КС

Основна ідея дедуктивного методу полягає в аналізі зіставлення вхідних і вихідних даних кіберсистеми з метою виявити деструктивні проникнення або уразливості шляхом виконання процедур порівняння між свідомо штатними (функціональними) режимами і ситуаціями, що викликають підозру. Для імплементації методу в інфраструктуру захисних сервісів необхідно мати графову модель логіки функціонування кіберсистеми, яка досить просто може бути трансформована до системи логічних рівнянь, придатної для дедуктивного аналізу. Далі пропонується модель дедуктивно-паралельного синхронного аналізу вразливостей (проникнень) кіберсистеми (об'єкта), яка дозволяє за одну ітерацію обробки структури обчислити всі деструктивні компоненти, що перевіряються на тест-векторі. Мета дедуктивного аналізу – визначити якість синтезованого тесту щодо повноти покриття їм вразли-

востей, а також побудувати таблицю перевірки тестовими наборами усіх виявлених вразливостей КС для виконання процедур діагностування. Така модель заснована на рішенні рівняння:

$$L = T \oplus F, \quad (1)$$

де F = (Fm+1, Fm+2, ..., Fi, ..., Fn), i = m+1, ..., n – сукупність функцій справної (коректної) поведінки КС; m – число його входів; Yi=Fi(Xi1, ..., Xij, ..., Xini) – ni-входовий i-й елемент схеми, що реалізує Fi для визначення стану лінії (виходу) Yi на тест-векторі Tt; тут Xij – j-й вхід i-го елемента; тест T=(T1, T2, ..., Tt, ..., Tk) – упорядкована сукупність двійкових векторів, визначена в процесі справного моделювання на множині вхідних, внутрішніх і вихідних ліній, об'єднана в матрицю

$$T = [T_{ti}] = \begin{bmatrix} T_{11}, T_{12}, ..., T_{1i}, ..., T_{1n} \\ ..... \\ T_{t1}, T_{t2}, ..., T_{ti}, ..., T_{tn} \\ ..... \\ T_{k1}, T_{k2}, ..., T_{ki}, ..., T_{kn} \end{bmatrix}, \quad (2)$$

невхідна координата якої визначається моделюванням функції Tti = Yi = Fi (Xi1, ..., Xij, ..., Xini) на тест-векторі Tt;

$$L = (L_1, L_2, ..., L_t, ..., L_k)$$

– множина дедуктивних схем або моделей, які визначаються виразом (3), де

$$L_t = (L_{t1}, L_{t2}, ..., L_{ti}, ..., L_{tn}); \quad L_{ti} = T_t \oplus F_i \quad (3)$$

– дедуктивна функція (ДФ) паралельного моделювання несправностей на тест-векторі T_t, відповідна справному елементу F_i, яка дає можливість обчислювати список вхідних проникнень, що транспортуються на вихід елемента F_i [17].

Поняття синхронності введеної моделі (1) визначається умовою:

$$\Delta t = (t_{j+1} - t_j) >> \tau >> \tau_i,$$

коли інтервал часу між зміною вхідних наборів (t_{j+1}–t_j), що подаються на КС, набагато більший від максимальної затримки системи τ і елемента τ_i. Це дозволяє виключити час як несуттєвий параметр [17], що використовується в технологіях моделювання та синтезу тестів.

У загальному випадку, коли функція КС представлена таблицею істинності, застосування формули (1) дозволяє отримати для заданого тест-вектора T_t таблицю транспортування вразливостей (проникнень), по якій можна записати ДФ моделювання деструктивностей. Приклади отримання таких функцій представлені в такому вигляді (перший доданок – тест-вектор, другий і результат – таблиці істинності і транспортування вразливостей):

X_1	X_2	Y_1
0	1	0

$\oplus$

X_1	X_2	Y_1
0	0	0
0	1	0
1	0	1
1	1	1

$=$

X_1	X_2	L_1
0	1	0
0	0	0
1	1	1
1	0	1

$L_1 = X_1X_2 \vee X_1\overline{X}_2;$

X_1	X_2	Y_2
1	1	1

$\oplus$

X_1	X_2	Y_2
0	0	0
0	1	0
1	0	0
1	1	1

$=$

X_1	X_2	L_2
1	1	1
1	0	1
0	1	1
0	0	0

$L_2 = X_1X_2 \vee X_1\overline{X}_2 \vee \overline{X}_1X_2.$

Тут дедуктивні функції L1, L2 записані у вигляді диз'юнктивної нормальної форми по конституентах одиниці таблиць транспортування деструктивностей.

З урахуванням розбиття тесту на складові вектори рівняння (1) отримання ДФ для Tt∈T приймає такий вигляд: Lt=Tt⊕F. Якщо функціональний опис КС представлено компонентами (примітивами), що формують стани всіх ліній (з'єднань) КС, то як формула перетворення справної моделі примітива Fi на тест-векторі Tt в дедуктивну функцію Lti виступає такий вираз:

$$L_{ti} = T_t \oplus F_i = f_{ti}[(X_{i1} \oplus T_{t1}), (X_{i2} \oplus T_{t2}), ..., (X_{ij} \oplus T_{tj}), ..., (X_{in_i} \oplus T_{tn_i})] \oplus T_{ti}, \quad (4)$$

який є основою дедуктивного аналізу деструктивних порушень КС [3, 6].

Приклад 4. Отримати дедуктивні функції паралельного моделювання вразливостей на вичерпному тесті для базису функціональних елементів And, Or, Not. З урахуванням виразу (4) виконуються такі очевидні перетворення для функції And:

$$L_{and}[T = (00,01,10,11), F = (X_1 \wedge X_2)] =$$
$$= L\{(\overline{x}_1\overline{x}_2 \vee \overline{x}_1x_2 \vee x_1\overline{x}_2 \vee x_1x_2) \wedge [(X_1 \oplus T_{t1} \wedge X_2 \oplus T_{t2}) \oplus T_{t3})]\} =$$
$$= (\overline{x}_1\overline{x}_2)\{[(X_1 \oplus 0) \wedge (X_2 \oplus 0)] \oplus 0\} \vee (\overline{x}_1x_2)\{[(X_1 \oplus 0) \wedge (X_2 \oplus 1)] \oplus 0\} \vee$$
$$\vee (x_1\overline{x}_2)\{[(X_1 \oplus 1) \wedge (X_2 \oplus 0)] \oplus 0\} \vee (x_1x_2)\{[(X_1 \oplus 1) \wedge (X_2 \oplus 1)] \oplus 1\} =$$
$$= (\overline{x}_1\overline{x}_2)(X_1 \wedge X_2) \vee (\overline{x}_1x_2)(X_1 \wedge \overline{X}_2) \vee (x_1\overline{x}_2)(\overline{X}_1 \wedge X_2) \vee (x_1x_2)(X_1 \vee X_2).$$

Аналогічно виконуються обчислення для функції Or:

$$L_{or}[T = (00,01,10,11), F = (X_1 \vee X_2)] =$$
$$= L\{(\overline{x}_1\overline{x}_2 \vee \overline{x}_1x_2 \vee x_1\overline{x}_2 \vee x_1x_2) \wedge [(X_1 \oplus T_{t1} \vee X_2 \oplus T_{t2}) \oplus T_{t3})]\} =$$
$$= (\overline{x}_1\overline{x}_2)\{[(X_1 \oplus 0) \vee (X_2 \oplus 0)] \oplus 0\} \vee (\overline{x}_1x_2)\{[(X_1 \oplus 0) \vee (X_2 \oplus 1)] \oplus 1\} \vee$$
$$\vee (x_1\overline{x}_2)\{[(X_1 \oplus 1) \vee (X_2 \oplus 0)] \oplus 1\} \vee (x_1x_2)\{[(X_1 \oplus 1) \vee (X_2 \oplus 1)] \oplus 1\} =$$
$$= (\overline{x}_1\overline{x}_2)(X_1 \vee X_2) \vee (\overline{x}_1x_2)(\overline{X}_1 \wedge X_2) \vee (x_1\overline{x}_2)(X_1 \wedge \overline{X}_2) \vee (x_1x_2)(X_1 \wedge X_2).$$

Тут $T_t=(T_{t1}, T_{t2}, T_{t3})$, t=1,2,3,4 – тест-вектор, який має 3 координати, де остання з них визначає стан виходу двохвходового елемента And (Or). У наступному перетворенні $T_t=(T_{t1}, T_{t2})$, t=1,2 – тест-вектор,

який має 2 координати, де друга – стан виходу інвертора:

$$L_{not}[T=(0,1), F=\overline{X}_1] = L\{(\overline{x}_1 \vee x_1)[(\overline{X_1 \oplus T_{t1}}) \oplus T_{t2}]\} =$$

$$= \overline{x}_1[(\overline{X_1 \oplus 0}) \oplus 1] \vee x_1[(\overline{X_1 \oplus 1}) \oplus 0] = \overline{x}_1 \overline{\overline{X}}_1 \vee x_1 \overline{\overline{X}}_1 = \overline{x}_1 X_1 \vee x_1 X_1.$$

Останній вираз ілюструє інваріантність інверсії до вхідного набору для транспортування вразливостей. Вона трансформується в повторювач. Тому дана функція не фігурує на виходах дедуктивних елементів. Спільна апаратурна реалізація ДФ для решти двохвходових елементів And, Or на вичерпному тесті представлена універсальним функціональним примітивом (рис. 8) дедуктивно-паралельного аналізу несправностей.

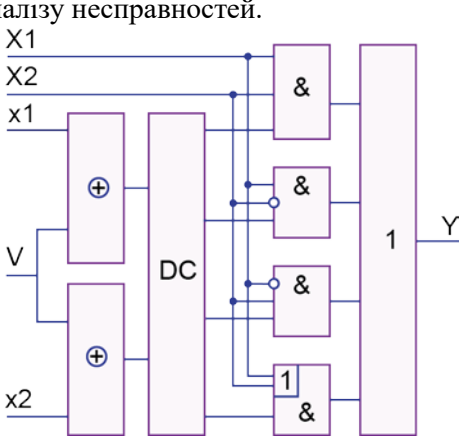

Рис. 8. Симулятор несправних примітивів

У симуляторі представлені булеві (x1, x2) і реєстрові (X1, X2) для кодування вразливостей входи, змінна вибору типу справної функції (AND, OR), вихідна реєстрова змінна Y. Стани двійкових входів x1, x2 і змінна вибору елемента визначають одну з чотирьох дедуктивних функцій для отримання вектора Y перевірки несправностей.

Для ілюстрації паралельного моделювання вхідних 8-розрядних векторів вразливостей в цілях отримання на виході Y множини перевірки деструктивниостей для логічних елементів 2And, 2Or використовується така таблиця:

(V, x1, x2) =	000	100	011	111	010	110
X1(RG)	01110001	01110001	10110110	00111011	00101010	10111001
X2(RG)	01111000	01111000	10110101	00110100	10111001	00101010
Y(RG)	01110000	01111001	10110111	00110000	10010001	10010001

Застосування такого симулятора дає можливість трансформувати функціональну модель F коректної поведінки КС в дедуктивну L, яка інваріантна в сенсі універсальності тестовим наборам і не передбачає в процесі моделювання використовувати модель F. Тому симулятор, як апаратна модель ДФ, є ефективним двигуном дедуктивно-паралельного моделювання КС, що підвищує швидкодію аналізу кіберсистем в 10 – 1000 разів у порівнянні з програмною реалізацією. Але при цьому співвідношення обсягів моделей коректного моделювання та аналізу вразливостей становить 1:10. Підхід апаратного аналізу деструктивний, спрямований на розширення функціональних можливостей вбудованих засобів моделювання, які можна зберігати на хмарі і постійно ними користуватися для верифікації інфраструктури захисту КС. Обчислювальна складність обробки проекту $Q=(2n^2r)/W$, де r – час виконання регістрової операції (And, Or, Not); W – розрядність регістра.

Для апаратної реалізації дедуктивно-паралельного моделювання на основі запропонованого симулятора може бути використана обчислювальна структура, представлена на рис. 9. Особливість схемної реалізації полягає в спільному виконанні двох операцій: однобітових – для емуляції функцій логічних елементів And, Or і паралельної – для обробки багаторозрядних векторів несправностей шляхом виконання операцій логічного множення, заперечення і складання.

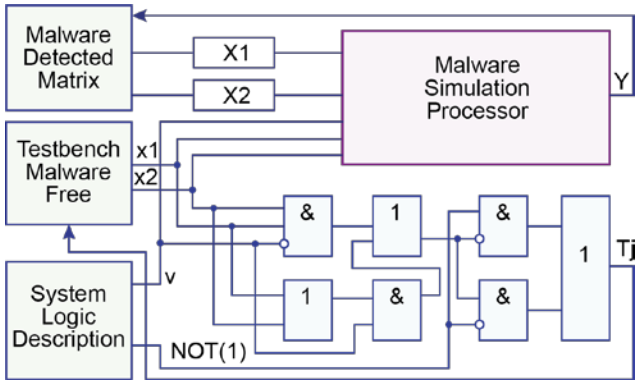

Рис. 9. HFS-структура апаратного моделювання

Функціональне призначення основних блоків (пам'ять і процесор): 1. $M=[M_{ij}]$ – квадратична матриця моделювання деструктивних проникнень (ДП), де i, j = 1, q; q – загальне число ліній в оброблюванsq КС. 2. Вектори збереження станів коректного моделювання, визначені в моменти часу t-1 і t, необхідні для формування дедуктивних функцій примітивів. 3. Модуль пам'яті для зберігання опису КС у вигляді структури логічних елементів. 4. Буферні регістри, розмірністю q, для зберігання операндів і виконання регістрових паралельних операцій над векторами ДП, що зчитані з матриці M. 5. Блок коректного моделювання для визначення двійкового стану виходу чергового оброблюваного логічного елемента. 6. Дедуктивно-паралельний симулятор, що обробляє за один такт дві реєстрових змінних X1, X2 з метою визначення вектора ДП, що транспортуються на вихід логічного елемента Y.

Перевага запропонованої структури моделювання ДП. 1. Суттєве зменшення кількості модельованих ДП, які визначаються тільки числом збіжних розгалужень, що становить до 20% від загального числа ліній. 2. Зниження обсягу пам'яті, необхідного для зберігання матриці модельованих ДП. 3. Простота реалізації Hardware Vulnerability Simulator (HVS) в апаратному виконанні, що дозволяє на порядок збільшити швидкодію моделювання ДП. 4. Використання HVS в якості першої фази дедуктивно-топологічного методу, який грунтується на результаті обробки розгалужень, що сходяться, для швидкодіючого аналізу деревоподібних структур.

Маршрут моделювання КС з попереднім розбиттям моделі пристрою на дві структурні частини (розгалуження, що сходяться, і деревовидні підграфи) представлений на рис. 10.

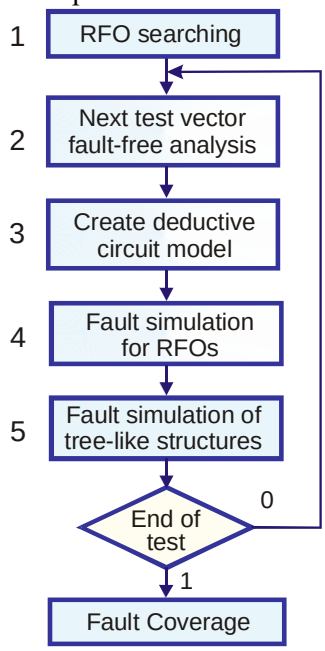

Рис. 10. Модель процесу дедуктивно-паралельного моделювання

Підсумки запропонованої технології моделювання з попередніми розбиттям КС на розгалуження, що сходяться, і деревовидні підграфи. Дедуктивно-паралельний аналіз ДП на основі їх зворотного простежування вимагає практично лінійних витрат пам'яті і часу, що залежать від числа ліній КС. Витрати часу для обробки розгалужень, що сходяться, мають квадратичну залежність від їх числа:

$$Q = (r^2 / W) + n_r + n_p + (n - r - r^0).$$

Тут (r^2 / W) – час моделювання ДП r розгалужень, що сходяться, число яких визначається як $r=0.2\times n$, $n_r=n$ – час реконфігурування примітивів схеми на вхідному наборі; $n_p = n$ – час пошуку підграфів ліній, відповідних неперевірюваним розгалуженням, що збігаються;

$$(n - r - r^0) = n - 0.2\times n - 0.4\times n = 0.4\times n$$

– час виконання суперпозиції рішень на множині ліній КС без сходяться розгалужень і попередників для непроверяемих сходяться розгалужень. З огляду на значення параметрів функції від числа ліній, можна отримати оцінку швидкодії дедуктивно-паралельного методу [14 – 16]:

$$Q = [(0.2\times n)^2 / W] + n + n + (n - 0.2\times n - 0.4\times n) = [(0.2\times n)^2 / W] + 2.4\times n).$$

Таким чином, виграш у швидкодії запропонованого методу тим більший, чим менший відсоток розгалужень, що сходяться, в КС.

Для порівняння: паралельний алгоритм має обчислювальну складність Ср, яка визначається функціональною залежністю від числа нееквівалентних ДП (b), довжини комп'ютерного слова (W), кількості еквівалентних вентилів (G):

$$C_p = (b^2 / W)\times G^3.$$

Дедуктивний алгоритм має відмінності у формулі оцінки швидкодії:

$$C_d = b^2 \times Q \times G^2\big|_{Q=G} = b^2 G^3,$$

де Q – середнє число активізованих ДП вентилів. Дедуктивно-паралельний метод без розбивки схеми має швидкодію, що визначається виразом:

$$C_{dp} = G^2 + (b^2 / W)\times G^2.$$

Перший доданок задає час коректного моделювання, другий – час аналізу ДП, лінії якого не ранжовані. Для комбінаційної ранжованої структури швидкодія методу має оцінку

$$C^r_{dp} = G + (b^2 / W)\times G.$$

Швидкодія дедуктивно-паралельного методу вища паралельного і дедуктивного

$$(C^r_{dp} << \{C_p, C_d\}),$$

завдяки поділу фаз коректного і ДП моделювань.

Запропонована технологія програмно-апаратного дедуктивно-паралельного моделювання ДП орієнтована на створення моделей дедуктивних примітивів компонентів і зв'язків КС з метою тестування вразливостей (проникнень). Представлена структурна модель апаратного симулятора і пристрої моделювання в цілому, які орієнтовані на істотне підвищення швидкодії засобів моделювання КС великої розмірності шляхом поділу функцій коректного аналізу і обчислення списків перевірки вразливостей на тестових наборах.

Метод дедуктивно-паралельного моделювання дає можливість оцінювати якість (повноту) запропонованих тестів, а також визначати всі потенційно можливі місця існування вразливостей в цілях їх подальшого усунення.

7. Висновки

1. Визначено компоненти блокчейн технології, які використовуються для створення надійної інфраструктури захисту даних, складеної з ненадійних елементів.

2. Представлена структурна модель відносин на безлічі з чотирьох основних компонентів тестування і діагностики (функціональність, КС, тест, уразливості), яка характеризується повною хогвзаємодією всіх вершин графа і транзитивною оборотністю кожної тріади відносин, що дозволяє визначити і класифікувати шляхи вирішення практичних завдань, включаючи синтез тестів, моделювання та пошук вразливостей.

3. Запропоновано вдосконалені методи синтезу тестів для функціональностей, заданих матричними формами опису поведінки компонентів КС, які відрізняються паралелізмом векторних операцій над таблицями, що дає можливість істотно (x2) підвищити швидкодію обчислювальних процедур.

4. Процес-моделі і методи синтезу тестів для функціональностей і діагностування ФН можуть бути використані як вбудовані компоненти інфраструктури сервісного обслуговування КС із застосуванням стандартів тестопридатності.

Література:

1. https://www.forbes.com/sites/louiscolumbus/2017/08/15/gartners-hype-cycle-for-emer-ging-technologies-2017-adds-5g-and-deep-learning-for-first-time/#646a4cf34be2

2. http://www.gartner.com/newsroom/id/3784363

3. http://www.wired.co.uk/article/ai-neuromorphic-chips-brains

4. *Gupta A. and Jha R. K.,* "A Survey of 5G Network: Architecture and Emerging Technologies," in IEEE Access, vol. 3, pp. 1206-1232, 2015.

5. *Zhu C., Leung V. C. M., Shu L. and Ngai E. C. H.,* "Green Internet of Things for Smart World," In *IEEE Access*, vol. 3, pp. 2151-2162, 2015.

6. *Christidis K. and Devetsikiotis M.,* "Blockchains and Smart Contracts for the Internet of Things," In *IEEE Access*, vol. 4, pp. 2292-2303, 2016.

7. *Blockchains*: How They Work and Why They'll Change the World IEEE Spectrum. October 2017. https://spectrum.ieee.org/computing/networks/blockchains-how-they-work-and-why-theyll-change-the-world

8. *Zanella A A., Bui N., Castellani A., Vangelista L. and Zorzi M.,* "Internet of Things for Smart Cities," In IEEE IoT Journal, vol. 1, no. 1, pp. 22-32, Feb. 2014.

9. https://www.gartner.com/doc/3471559?srcId=1-7578984202&utm_campaign=RM_GB_2017_TRENDS_QC_E2_What&utm_medium=email&utm_source=Eloqua&cm_mmc=Eloqua-_-Email-_-LM_RM_GB_2017_TRENDS_QC_E2_What-_-0000

10. http://www.gartner.com/smarterwithgartner/three-digital-marketing-habits-to-break-2/

11. *Vladimir Hahanov,* Cyber Physical Computing for IoT-driven Services, New York, Springer, 2017. 259 p.

12. *Laura Shin.* Buying Bitcoin and Other Crypto Assets // Forbes Newsletters. 2018. 6 p. [http://info.forbes.com/rs/790-SNV-353/images/crypto.pdf?mkt_tok=eyJpIjoiWVdOalltVTRN-VEppWmpaaSIsInQi-OiJkb2lLYWE1djgyV3laRkRseWh1MlNGc1N2S3hTVkF-HejNDT0ZDZzV4RFA0MlV2cmRpMHNjNEp6MkU5S0VsSU1xUTRNd0RpeStQMGJ5SUd-NWTMramdBTkV4V3FSY1JcL0VGYTRrcXNnTVFvMG1jdldEZ1RFcTkyWHhKQUZGZzVWb1oifQ%3D%3D]

13. https://spectrum.ieee.org/tech-talk/computing/networks/quantum-blockchains-could-act-like-time-machines?utm_source=computingtechnology&utm_campaign= computingtechnology-05-01-18&utm_medium=email

14. *Hahanov V., Wajeb Gharibi, Litvinova E., Chumachenko S.* Information analysis infrastructure for diagnosis // Information an international interdisciplinary journal. 2011. Japan. Vol.14. № 7. P. 2419-2433.

15. *Bau Jason, Bursztein Elie, Gupta Divij, Mitchell John.* State of the Art: Automated Black-Box Web Application Vulnerability Testing // 2010 IEEE Symposium on Security and Privacy. 2010. P. 332 – 345.

16. *Shahriar H., Zulkernine M.* Automatic Testing of Program Security Vulnerabilities // 33rd Annual IEEE International Computer Software and Applications Conference. 2009.Vol. 2. P. 550 – 555.

17. *Sedaghat S., Adibniya F., Sarram M.-A.* The investigation of vulnerability test in application software // International Conference on the Current Trends in Information Technology (CTIT). 2009. P.1 – 5.

18. *Хаханов В.И., Anders Carlsson, Чумаченко С.В.* Инфраструктура pentesting и управления уязвимостью // Автоматизированные системы управления и приборы автоматики. 2012. Вып. 160. С. 36-54.

Надійшла до редколегії 17.12.2018

Рецензент: д-р техн. наук, проф. Дрозд О.В.

Адамов Олександр Семенович, старший викладач кафедри АПОТ ХНУРЕ. Наукові інтереси: кібербезпека. Адреса: Україна, 61166, Харків, пр. Науки, 14, тел. 70-21-326. E-mail: oleksandr.adamov@nure.ua.

Хаханов Володимир Іванович, д-р техн. наук, професор кафедри АПОТ ХНУРЕ. Наукові інтереси: технічна діагностика цифрових систем, мереж і програмних продуктів. Захоплення: баскетбол, футбол, гірські лижі. Адреса: Україна, 61166, Харків, пр. Науки, 14, тел. 70-21-326. E-mail: hahanov@nure.ua.

Чумаченко Світлана Вікторівна, д-р техн. наук, професор кафедри АПОТ ХНУРЕ. Наукові інтереси: математичне моделювання, теорія рядів, методи дискретної

оптимізації. Захоплення: подорожі, аматорське фото. Адреса: Україна, 61166, Харків, пр. Науки, 14, тел. 70-21-326. E-mail: Svetlana.Chumachenko@nure.ua.

Абдуллаєв Вугар Гаджімахмудович, канд. техн. наук, доцент кафедри «Комп'ютерна інженерія технології та програмування» Азербайджанської Депржавної Нафтової Академії (АГНА), Інститут Кібернетики. Наукові інтереси: інформаційні технології, веб-програмування, мобільні додатки. Захоплення: електронна комерція, B2B, B2C проекти, наукові книги, спорт. Адреса: Азербайджан, AZ1129, Баку, вул. М. Гаді, 53, кв. 81, тел. (99412) 5712428, (050) 3325483, e-mail: abdul-vugar@mail.com

Adamov Aleksandr Semenovich, Senior Lecturer, Design Automation Department, NURE. Scientific interests: cybersecurity. Address: Ukraine, 61166, Kharkiv, Nauki Avenue, 14, tel. 70-21-326. E-mail: oleksandr.adamov@nure.ua.

Hahanov Vladimir Ivanovich, Dr. Tech. Sciences, professor, Design Automation Department, NURE. Scientific interests: technical diagnosis of digital systems, networks and software products. Hobbies: basketball, football, mountain skiing. Address: Ukraine, 61166, Kharkiv, Nauki Avenue, 14, tel. 70-21-326. E-mail: hahanov@nure.ua.

Chumachenko Svetlana Viktorovna, Dr. Tekhn. Sciences, professor, head of Design Automation Department, NURE. Scientific interests: mathematical modeling, series theory, discrete optimization methods. Hobbies: travel, amateur photo. Address: Ukraine, 61166, Kharkiv, Nauki Avenue, 14, tel. 70-21-326. E-mail: Svetlana.Chumachenko@nure.ua.

Abdullaev Vugar Gadzhimakhmudovich, Cand. tech. Sci., Associate Professor of Computer Engineering and Technology Programming at the Azerbaijan State Oil Academy (ASAN), Institute of Cybernetics of ANAS. Scientific interests: information technology, web programming, mobile application. Hobbies. e-commerce, B2B, B2C projects, science books, sports. Address: Azerbaijan, AZ1129, Baku, M. Gadi, 53, apt. 81, tel. (99412) 5712428, (050) 3325483, e-mail: abdulvugar@mail.com