УДК 004.891

к.т.н., доц. **Муляр І.В.** (ХмНУ)
к.т.н., с.н.с. **Мірошніченко О.В.** (ВІКНУ)
к.т.н., с.н.с. **Краснік А.В.** (ВІКНУ)
Солодєєва Л.В. (ВІКНУ)

ЗАХИСТ ВІД ПРИХОВАНИХ ЗАГРОЗ В СЕРЕДОВИЩІ ХМАРНИХ ОБЧИСЛЕНЬ

Наявність гіпервізорів в середовищі хмарних обчислень створює новий клас загроз, реалізація яких пов'язана з неоднозначністю переходів між різними рівнями ієрархії.

Застосування сучасних технологій адаптивних систем захисту інформації не дозволяє здійснювати повний контроль за інформаційними потоками середовища хмарних обчислень, оскільки вони функціонують на верхніх рівнях ієрархії. Тому для створення ефективних механізмів захисту ПЗ в середовищі хмарних обчислень потрібна розробка нових моделей загроз і створення методів відображення комп'ютерних атак, які дозволяють оперативно ідентифікувати приховані і потенційно небезпечні процеси інформаційної взаємодії.

Автором розроблена модель прихованих загроз інформаційній безпеці в середовищі хмарних обчислень, що враховує активний характер суб'єктів і об'єктів інформаційної взаємодії.

Також розроблена модель операцій, що відбуваються з даними при їх обробці в середовищі хмарних обчислень, що дозволяє формалізувати опис інформаційних процесів у вигляді мультиграфа транзакцій.

Суть пропонованого підходу полягає в представленні прихованої загрози у вигляді функції предикатів, змінні якої явно ініціалізуються. Функція предикатів вирішувана для всіх наборів змінних. Рішення задачі протидії прихованим загрозам формалізується з використанням набору предикатів, що дозволяє представити функції оцінки допустимості переходів в мультиграфі транзакцій у вигляді набору таблиць правил політики безпеки.

Правила розмежування доступу, складають основу політики безпеки, включають і обмеження на механізми ініціалізації процесів доступу. В рамках розробленої моделі операцій формалізований опис прихованих загроз зводиться до появи контекстно-залежних переходів в мультиграфі транзакцій.

Ключові слова: гіпервізор, хмарні обчислення, кібербезпека, приховані загрози.

Вступ. Розповсюдження мереж з високою потужністю, низька вартість комп'ютерів і пристроїв зберігання даних, а також широке впровадження віртуалізації, сервіс-орієнтованої архітектури привели до величезного зростання хмарних обчислень. Хмарні обчислення — це модель забезпечення зручного доступу на вимогу через мережу до обчислювальних ресурсів, які можуть бути оперативно надані та звільнені з мінімальними управлінськими затратами та зверненнями до провайдера.

Середовище хмарних обчислень - це сукупність обчислювальних ресурсів у вигляді віртуальних машин, що надаються користувачеві за допомогою загальних сервісів доступу. Фізичний рівень хмарної системи складається з апаратних ресурсів, які необхідні для забезпечення сервісів, що надаються, і, як правило, включає сервери, системи зберігання і мережеві компоненти. Застосування технологій хмарних обчислень визначає необхідність розгляду можливих способів дестабілізуючих дій, що приводять до порушення функціонування компонентів інформаційного середовища.

Розвиток мережевих технологій в напрямку створення середовищ хмарних обчислень (СХО) пред'являє нові вимоги до засобів розмежування доступу до інформаційних сервісів – одному з основних компонент сучасної системи інформаційної безпеки. Ці вимоги випливають з необхідності врахування динамічного характеру процесів виділення обчислювальних і мережних ресурсів при конфігурації віртуальних машин і структури адресного простору, використовуваного для доступу до інформаційних сервісів. Опис політики доступу може бути представлено за допомогою правил фільтрації мережевого трафіка, структура і параметри яких генеруються в процесі функціонування середовища хмарних обчислень і сервісів, що реалізуються з використанням віртуальних машин (ВМ). При

цьому необхідно враховувати вимоги збереження цілісності політики доступу, аналогічно тому, як в умовах зміни мережевої топології для збереження інформаційної зв'язності ресурсів в Інтернеті використовуються протоколи динамічної маршрутизації. При використанні СХО для розміщення інформаційних сервісів особливу актуальність набуває складна науково-технічна задача розвитку технологій захисту інформації, що забезпечує виконання вимог політики доступу в мережевому середовищі з динамічно змінними характеристиками.

Характерною особливістю сучасного середовища хмарних обчислень є активний характер суб'єктів і об'єктів інформаційної взаємодії. Це дозволяє розглядати цільову функцію системи безпеки як збереження конфіденційності, цілісності і доступності програмних і інфраструктурних сервісів, що надаються в режимі видаленого доступу в умовах динамічної зміни стану обчислювальних ресурсів. Побудова перспективних механізмів забезпечення безпеки в середовищі хмарних обчислень зв'язується не із захистом від виявлених вразливостей, а полягає в можливості запобігання новим невідомим методам проведення атак, в розробці нових моделей загроз і методів запобігання або віддзеркалення комп'ютерних атак на інформаційні ресурси, які використовують можливості предикативної ідентифікації прихованих каналів і потенційно небезпечних процесів інформаційної взаємодії [1].

Перспективним напрямком вирішення сформульованої задачі є використання технології між мережевого екранування з урахуванням специфіки захищеності середовища [2]. Для цього необхідна формалізація вимог розмежування доступу до інформаційних сервісів. Така формалізація може бути представлена з використанням динамічно формованого набору правил фільтрації, що забезпечує виконання вимог політики доступу. При цьому зростаюча складність алгоритмів фільтрації пред'являє високі вимоги до продуктивності між мережевих екранів, що робить необхідним використання методів паралельної обробки віртуальних з'єднань за допомогою віртуальних машин. У сучасній літературі підхід до створення складних технічних систем, зв'язаність яких забезпечується за рахунок організації процесів обміну інформацією з мережі, отримав назву мережево-центричний. Цей підхід стосовно задачі розмежування доступу вимагає забезпечення ситуаційної обізнаності та локальності дій кожного з між мережевих екранів, що входять до складу віртуальних машин, які використовуються в СХО для реалізації політики доступу [3].

Важливим напрямом вдосконалення технологій захисту і систем інформаційної безпеки є протидія білатеральним загрозам, в яких суб'єкт і об'єкт процесів інформаційної взаємодії є потенційним носієм небезпечних дій. У таких випадках необхідно використовувати моделі загроз, які ідентифікують потенційні вразливості як на рівні процесів контролю доступу до ресурсів гостьових операційних систем (ОС) або додатків, так і на рівні системних викликів гіпервізора, який сам може стати джерелом руйнуючих дій що реалізовуються шляхом порушення функціонування планувальника завдань або диспетчера устаткування. Загрози, що виникають при цьому, необхідно не тільки оперативно виявляти, але і блокувати використовувані неавторизовані канали інформаційних дій, які в середовищі хмарних обчислень зазвичай реалізуються в прихованому для гостьових ОС режимах. Тому важливим чинником підвищення ефективності систем захисту від прихованих загроз є облік напряму передачі, синтаксису і контексту потоків даних, які передаються [4].

З врахуванням вищесказаного, захист від загроз, які можуть приводити до розкрадання даних, неконтрольованої модифікації програмного коду, порушенню доступності (блокуванню) або нав'язуванню помилкової інформації в середовищі хмарних обчислень є актуальним науково-технічним завданням, вирішенню якого присвячена дана магістерська робота [5].

Постановка задачі. Використання традиційних підходів не дозволяє вирішити проблему підвищення рівня захищеності середовища хмарних обчислень з урахуванням гнучкості, масштабованості (підтримка апаратних платформ різного класу) пропонованих програмно-технічних рішень і мінімізації витрат.

Застосування сучасних технологій адаптивних систем захисту інформації не дозволяє здійснювати «прозорий» контроль за інформаційними потоками середовища хмарних обчислень, оскільки вони функціонують на верхніх рівнях ієрархії.

Класичні методи пошуку шкідливого програмного коди не дозволяють виявляти нові зразки шкідливого ПО, що реалізовує технології DKOM і VICE, оскільки вони вбудовуються в операційну систем на «нижчому» рівні, ніж модулі адаптивних систем захисту [6].

Традиційні методи перехоплення системних функцій гостьових ОС не дозволяють виявляти програмні «закладки», що вшиваються в ОС на етапі завантаження.

Для боротьби з такими загрозами актуальною є розробка нових засобів захисту інформації, заснованих на методах оперативної ідентифікації потенційних вразливостей, що виникають як на рівні процесів контролю доступу до ресурсів гостьових ОС, так і на рівні системних викликів гіпервізора, які за певних умов самі можуть ставати джерелами різних видів руйнівних впливів. Метою дослідження є підвищення рівня захищеності обчислювальних систем на основі розробки моделей, методів і алгоритмів протидії прихованим загрозам в середовищі хмарних обчислень.

Для досягнення поставленої мети вирішуються наступні завдання:

Розроблена модель прихованих загроз інформаційній безпеці в середовищі хмарних обчислень, що враховує активний характер суб'єктів і об'єктів інформаційної взаємодії.

Розроблена модель операцій, що відбуваються з даними при їх обробці в середовищі хмарних обчислень, що дозволяє формалізувати опис інформаційних процесів у вигляді мультиграфа транзакцій.

Розроблений метод протидії прихованим загрозам з використанням запропонованої моделі операцій, заснований на характеризації ієрархії транзакцій.

Виклад основного матеріалу. Розглянемо компоненти гіпервізора як джерело загрози при проведенні атак зловмисником з подальшим розповсюдженням шкідливого програмного забезпечення на серверах віртуалізації.

Користувачі можуть атакувати компоненти гіпервізора, посилаючи некоректні запити на обробку модулям програмного забезпечення гіпервізора і використовуючи недокументовані можливості системного і прикладного програмного забезпечення, встановленого на серверах віртуалізації. Логіка виконання програм повинна контролюватися з точки зору відмови в обслуговуванні. Це підвищує ризики при реалізації прихованих загроз, не тільки функціональних можливостей, але і безпеки, яка оцінюється величиною ризику їх не документованої роботи. Приховані загрози, що приводять до порушення роботи середовищі хмарних обчислень, реалізуються за допомогою дій з боку шкідливого програмного забезпечення, від яких немає захисту на рівні гостьової ОС [7].

Під реалізацією прихованих загроз маються на увазі використання механізмів створення і зміни контексту виконання потоків, за допомогою яких можуть передаватися дані від сутностей з високим рівнем безпеки до сутностей з низьким рівнем безпеки в обхід правил і може порушуватися стан захищеності самого гіпервізора.

Гіпервізор забезпечує ізоляцію різних ОС одна від одної, розділення і управління ресурсами. Гостьові ОС – це операційні системи віртуальних машин, що запускаються під управлінням гіпервізора.

У гіпервізорі, як і в будь-якій операційній системі, створюється множина сутностей (об'єктів і суб'єктів доступу) з різним рівнем безпеки. Операція породження суб'єктів $Create\left(Subi, Om\right) \to Subj$ називається породженням з контролем незмінності об'єкту, якщо для будь-якого моменту часу t > t0 , в який активізована операція породження об'єкту $Create$, породження об'єкту $Subj$ можливо тільки при тотожності об'єкту-джерела щодо моменту $t0 : Om[t] = Om[t0]$, де Sub – суб'єкт, O – об'єкт доступу. У разі середовища хмарних обчислень суб'єкти і об'єкти доступу можуть мінятися ролями [8].

Тому для протидії прихованим загрозам в середовищі хмарних обчислень, в якому діє породження суб'єктів з контролем незмінності об'єкту, необхідно, щоб у момент часу $t0$ через

будь-який суб'єкт до будь-якого об'єкту існували тільки потоки, що не суперечать умові коректності: монітор безпеки повинен реалізувати спеціальні механізми ідентифікації контексту контрольованих потоків даних як для суб'єктів, так і для об'єктів доступу, а будь-який суб'єкт доступу (ініціатор доступу) повинен використовувати тільки дозволені механізми доступу. З цією метою вводиться набір який підходить для створення об'єктів доступу, так і при породженні об'єктів у вигляді кортежу $(s, Ord, Context\_type)$, тобто формалізація операцій породження суб'єктів або об'єктів доступу представляється в наступному вигляді:

$$Create(Subi, Om, s, Ord, Context\_type) \to Subj, Create(Om, s, Ord, Context\_type) \to Oj. \quad (1)$$

При цьому породження нового суб'єкта доступу з номером j Sub_j можливо тільки за умови, що $Om[t] = O_m[to]$, де Sub - суб'єкт доступу, O_m - об'єкт доступу, j, m - номера об'єктів в запропонованій специфікації даного хмарного середовища.

Таблиці дозволених зв'язків об'єктів і суб'єктів доступу, за допомогою яких здійснюється контроль транзакцій операцій породження нових об'єктів, необхідно розширити на випадок прихованих загроз. Опис таблиці правил ПБ (політики безпеки) приведено в 3 розділі.

Предикативна функція ідентифікації прихованих загроз - це відображення 8-рівневої моделі операцій на множину його можливих станів - небезпечні, безпечні і невизначені. В цьому випадку модель прихованих загроз описується у вигляді розширеного кортежу:

$$M = \langle Source, Services, Devices, \{proc\}, Actions, \{hv\}, \{vm\}, Security\ Roles \rangle, \quad (2)$$

де $Source$ - суб'єкт доступу або процес, джерело загрози;

$Services$ - набір шаблонів правил безпеки, використовуваних традиційними СЗІ (наприклад, правила фільтрації для МСЕ тощо);

$Devices$ - пристрої, що встановлені на серверах віртуалізації і використовувані гостьовими операційними системами ВМ (диск, мережний контролер тощо), як об'єкт доступу;

$\{ proc \}$ - множина суб'єктів впливу (шкідливий код гіпервізора, несертифіковані засоби віртуалізації і. т. п.);

$Actions$ - (дії) виконання операцій суб'єктом по відношенню до об'єкту доступу (виконання команд read, write, append, create, execute…)

$\{hv\}$ - середовище взаємодії процесів ВМ у гіпервізорі, що представляє собою множину компонентів $\mathrm{mod}\, i$;

$\{vm\}$ - об'єкти впливу (множина ВМ).

- $Security - Roles$ - процедури багаторівневої рольової ПБ для протидії прихованим загрозам, які реалізуються у вигляді набору міток безпеки. Набір міток являють собою значення кортежу $(s, Ord, Context\_type)$..

В рамках пропонованої моделі загроз середовище хмарних обчислень розглядається як система взаємодії гіпервізорів, встановлених на серверах віртуалізації. В рамках направленої схеми «суб'єкт-дія-об'єкт» активний характер суб'єктів і об'єктів інформаційної взаємодії передбачає ту обставину, що вони можуть мінятися місцями. Розглянемо ситуацію, в якій зловмисник(суб'єкт) атакує сервер віртуалізації(об'єкт), модифікує компоненти гіпервізора шляхом реалізації нових загроз, приведених в таблиці 1.

Таблиця 1

Перелік нових загроз, які виникають в середовищі хмарних обчислень.

Перелік загроз	Наслідки
Загроза нестандартного виконання команд в гіпервізорі	Можливість отримання несанкціонованого доступу до ресурсів гіпервізора
Загроза порушення однозначності переходів станів при обміні інформацією між віртуальною машиною та гіпервізором	Можливість отримання несанкціонованого доступу до даних користувача іншої віртуальної машини
Загроза модифікації програмного забезпечення гіпервізорі	Поширення шкідливого програмного забезпечення в середовищі хмарних обчислень

Модель операцій, що виконуються на різних рівнях ієрархії середовища хмарних обчислень, дозволяє описати інформаційні процеси у вигляді мультиграфа транзакцій. Середовище виконання команд ВМ розглядається як 8-рівнева ієрархічна модель (рис. 1).

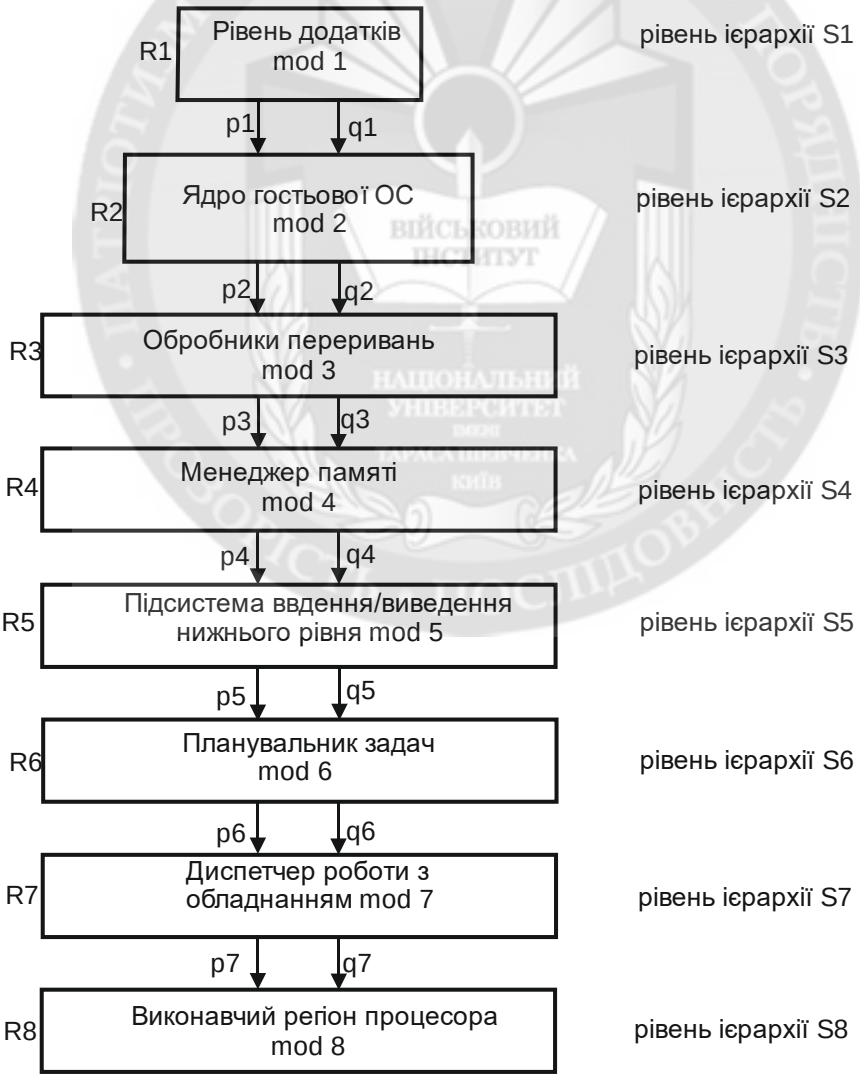

Рис. 1. Структура взаємодії процесів віртуальних машин в гіпервізорі

Існують 8 рівнів ієрархії: $S1$- рівень додатків; $S2$- рівень ядра гостьової ОС; $S3$ – рівень обробників переривань; $S4$- рівень менеджера пам'яті гіпервізора; $S5$ – рівень підсистеми-введення виведення гіпервізора; $S6$ – рівень планувальника завдань гіпервізора; $S7$ – диспетчер роботи з устаткуванням гіпервізора; $S8$ – рівень виконавчого регіону процесора. На рівнях $S1-S5$ функціонують традиційні СЗІ, які використовують набори шаблонів ПБ для контролю доступу. На рівнях $S6-S7$ шкідливим ПЗ реалізуються приховані загрози, про які згадувалося раніше. На рівні $S8$ здійснюється контроль виконання операцій ВМ з урахуванням вимог політики безпеки [9].

На основі комбінаторного аналізу можливих переходів при виникненні подій з множини E необхідно довести, що при числі рівнів ієрархії рівним 8 відображення $Si\ x\ Ei :\rightarrow Sj$. Якщо кількість рівнів менше 8, то відображення не ізоморфно. Кожному переходу відповідає набір ініціалізованих предикатів, Число всіх можливих підстановок предикатів у функцію оцінки допустимих станів рівне $n!$.

Пропонований підхід до опису операцій заснований на класифікації ризиків і на аналізі контексту виконання потоків команд, за допомогою яких можуть передаватися дані в обхід правил, що відповідають прийнятій ПБ, і порушують стан захищеності самого гіпервізора.

Таблиця 2

Опис рівнів захисту

Рівень захисту	*Зовнішні дії*	*Приклад шкідливого коду*
1 рівень – S1	VI, V2, V3	HackerDefender, Hox, Seven і бібліотеці AFX Rootkit
2 рівень – S2	V4, V5, V6	HackerDefender, Hox, Seven і бібліотеці AFX Rootkit
3 рівень – S3	V7,V8	Seven,Pandora
4 рівень- S4	V9,V10	Red Pill, Storm
5 рівень- S5	V11	Croax,Legend
6 рівень –S6	V12,V13,V14	Ice Brute, Dragon, FUTO
7 рівень – S7	V15 – перехоплення управління в режимі віртуалізації або налагоджувальної сесії	Blue Pill,RuStock 1, RuStockпрототипи майбутніх версій руткитов на основі технології DKOM (Direct Kernel Object Manipulation) і VICEirtual ICE
8 рівень –S8	На даному рівні потенційні дії виходять за рамки дій, які розпізнає шкідливий код	На даному рівні структура даних є не списком покажчиків, доступних для модифікації експортованими функціями ядра, а поіменованим набором всіх індексів (ідентифікаторів) потоків

Кожен компонент гіпервізора описується кінцевим автоматом

$$\mathrm{mod}_i = \left(Ei, Ri, start, \Pr ivi, Fi, Pi, Vi\right), \qquad (3)$$

де $\text{mod}_i \in M$ – множина всіх компонентів середовища взаємодії процесів ВМ; $Ei\, i\, Vi \in E$ – множина подій або вхідних дій, що змінюють стани компонентів гіпервізора;

початковий стан start при запуску ВМ;

$Fi : Ri\ x Vi \to Rj$ - функція переходу з стану Ri в Rj під зовнішньою дією Vi;

$\Pr ivi$ – рівень привілеїв в Ri стані, $\Pr ivj$ – рівень привілеїв в Rj стані, $Pi : Ri \to \{1 | 0\}$, Pi – функція допустимості стану, яка є кортежем простих предикатів

$$Pi = (s, Ord, Context\_type). \quad (4)$$

Функція Pi характеризує стани компонентів як дозволені або заборонені, де s – предикат, що визначає контекст виконання процесу (потоку):

$s = 0$ *якщо* $Max(\Pr ivi, \Pr ivj)$, - збільшення рівня привілегій;

$s = 1$ *якщо* $Min(\Pr ivi, \Pr ivj)$, - зменшення рівня привілегій;

Ord – предикат, задаючий ознаку батьківського або дочірнього процесу (потоку):

$Ord = 0$ - якщо процес батьківський;

$Ord = 1$ - якщо процес дочірній.

Предикатом $Context\_type$ є трійка $\{1 | 0 | -1\}$ і визначає зміни контексту виконання процесу(потоку):

- $Context\_type = 1$ відповідає операціям читання/запису в області пам'яті додатків;
- $Context\_type = -1$, здійснюються операції читання/запису в привілейовану область пам'яті пристроїв гостьової ОС;
- $Context\_type = 0$ режим очікування нових транзакцій, без здійснення операцій запису даних.

В рамках моделі операцій розглядаємо 4 рівні привілеїв : $\Pr iv0$ - рівень привілеїв команд процесора, $\Pr iv1$ - рівень привілеїв ядра ОС, $\Pr iv2$ - рівень привілеїв адміністратора безпеки сервера віртуалізації, $\Pr iv3$ - рівень привілеїв користувачів ВМ. З урахуванням того, що істотною особливістю операцій в середовищі хмарних обчислень є можливість зміни ролі суб'єктів і об'єктів інформаційної взаємодії, для контролю незмінності об'єктів пропонується використовувати спеціальні механізми ідентифікації контексту виконання процесів.

Контекст виконання запиту – це дерево реберних графів для кожного вузла мультиграфа транзакцій з ідентифікатором *context_id* і набором міток *s, Ord, Context_type*.

Суть пропонованого підходу полягає в представленні прихованої загрози у вигляді функції предикатів, змінні якої явно ініціалізуються. Функція предикатів вирішувана для всіх наборів змінних. Рішення задачі протидії прихованим загрозам формалізується з використанням набору предикатів, що дозволяє представити функції оцінки допустимості переходів в мультиграфі транзакцій у вигляді набору таблиць правил політики безпеки [9].

Правила розмежування доступу, складають основу політики безпеки, включають і обмеження на механізми ініціалізації процесів доступу. В рамках розробленої моделі операцій формалізований опис прихованих загроз зводиться до появи контекстно-залежних переходів в мультиграфі транзакцій.

Отже метод заснований на тому, що набір міток *{m}* для «розфарбовування» мультиграфа транзакцій представляється значеннями предикатів *s, Ord, Context_type*. Тому кожен запит користувачів ВМ до інформаційних ресурсів формально описується у вигляді кортежу предикатів і поля ідентифікатора *Context_id*. Зміна контексту виконання запиту формалізується у вигляді матриці інцидентності гіпервізора. Неоднозначність переходів пояснюється існуванням неконтрольованих станів.

Проте, як показано в розділі 2, пов'язані з цими станами функції предикатів вирішувані для всіх наборів контрольованих змінних. Тому разом з описом інформаційних процесів за допомогою мультиграфа транзакцій для кожного окремого процесу будується граф породжених ним процесів, які зв'язані загальним ідентифікаційним номером *Context_idi* і наборами міток.

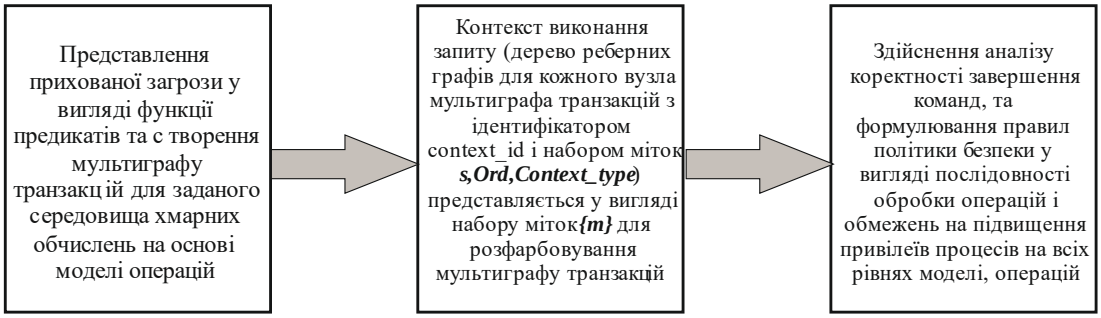

Рис. 2. Графічне представлення методу предикативної ідентифікації процесів для захисту від прихованих загроз

Обмеження на підвищення привілеїв і контроль переходів при зміні контексту операцій задаються значеннями кортежу предикатів *Pi. = (s, Ord, Context_type)*, а контроль виконання потоків, що породжуються суб'єктами доступу, реалізується на основі принципу найменших привілеїв [10].

На рис. 3 приведена схема роботи алгоритму предикативної ідентифікації прихованих загроз інформаційній безпеці в середовищі хмарних обчислень.

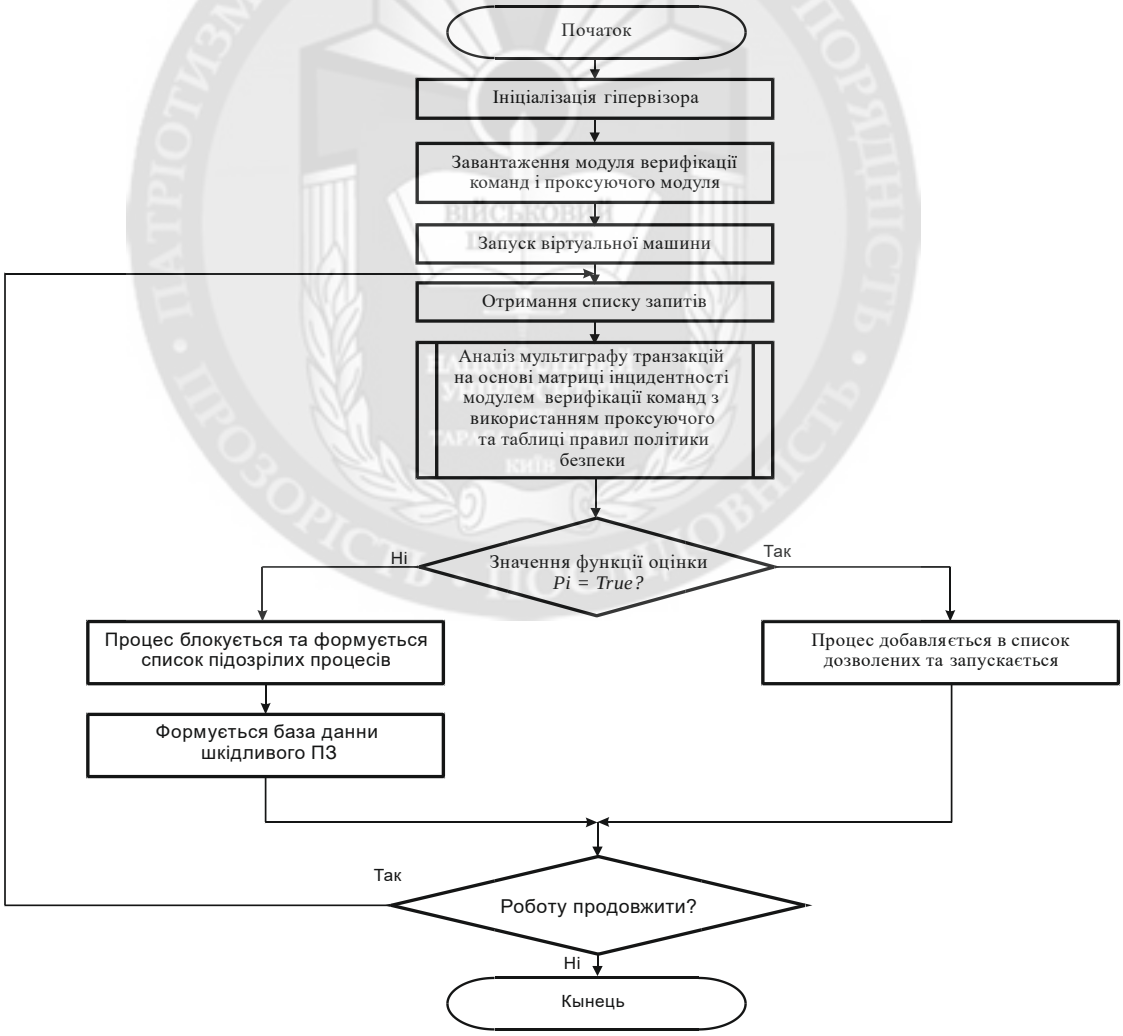

Рис. 3. Узагальнена блок-схема роботи алгоритму предикативної ідентифікації

Призначення алгоритму – виявлення шкідливого ПЗ в компонентах гіпервізора і гостьових ОС. Як вхідні параметри використовуються списки запитів від користувачів ВМ. Запитом користувачів є набір операцій. У середовищі хмарних обчислень користувачі взаємодіють з фізичним устаткуванням за допомогою гіпервізора. При цьому робота користувачів ВМ здійснюється з логічними пристроями, створюваними компонентами гіпервізора - програмними емуляторами, функціонуючими на рівнях *S3, S4, S5*. Програмні емулятори пристроїв обробляють системні виклики гостьових ОС, виділяють їм сторінки пам'яті і забезпечують виконання операцій введення-виводу нижнього рівня. Окрім програмних емуляторів пристроїв, до складу гіпервізора входять планувальник завдань (рівень *S6*), диспетчер по роботі з устаткуванням (рівень *S7*) і модуль для роботи з процесором, що підтримує повну апаратну віртуалізацію (рівень *S8*).

Початок роботи алгоритму – запуск ВМ і отримання списку запитів від користувачів віртуальних машин, які представляються певним набором операцій.

Процедура пошуку прихованих загроз є циклом, в якому аналізуються списки запитів, на основі значення функції оцінки стану *Pi*: якщо *Pi = true* – процес додається в список дозволених, якщо *Pi = false*, формується список підозрілих процесів. В результаті роботи алгоритму створюється база даних шкідливого ПЗ, яка періодично оновлюється.

Використання багатокритеріальних методів прийняття рішень є важливою процедурою при системному підході до побудови систем захисту [12].

Висновки. У будь-якій обчислювальній системі існують інтерфейсні рівні взаємодії між різними модулями(компонентами), що дозволяють використовувати недокументовані можливості, з одного боку, для проведення атак зловмисником, з іншої – для реалізації механізмів моніторингу з боку систем контролю і захисту ПЗ середовища хмарних обчислень.

Загроза порушення доступу до конфіденційної інформації породила необхідність розробки нових методів захисту ПЗ та предикативного алгоритму на основі розробленої моделі операцій, що допомагає систематизувати функціональні рівні, використовувані зловмисником для вбудовування до гостьової ОС і гіпервізора, і протидіяти впровадженню шкідливих кодів та загроз, які формують послідовності запитів до некоректних програмним модулів гіпервізора або використовують недекларовані можливості системного і прикладного програмного забезпечення. Різні компоненти гіпервізора розглядаються в якості потенційного джерела загроз кібербезпеці, які реалізується шляхом поширення шкідливого програмного забезпечення або ініціалізації процесів, що руйнують стан захищеності ресурсів середовища хмарних обчислень.

Застосування методу протидії прихованим загрозам на основі розробленої моделі операцій дозволяє за рахунок реалізації механізмів вбудовування в гіпервізор на рівнях S6, S7, S8, оперативно визначити наявність атаки із застосуванням новітніх «руткіт»-технологій і своєчасно прийняти адекватні заходи захисту.

ЛІТЕРАТУРА:

1. Муляр І.В. Аналіз проблем забезпечення функціональної безпеки інформаційних систем обробки даних / І.В. Муляр, А.В. Джулій, М.В. Костюк // Вимірювальна та обчислювальна техніка в технологічних процесах: Міжнародний науково-технічний журнал. – Хмельницький, 2013. – №1. – С. 133-138.

2.Моляков, А.С. KPROCESSOR_CID_TABLE факторинг – новый метод в теории компьютерного анализа вирусного кода и поиска программных закладок / А.С. Моляков // Проблемы информационной безопасности. Компьютерные системы. – СПб.: Изд-во Политех. Ун-та, 2009. – №1. – С. 17-19.

3. Гурман І.В. Метод адаптивної маршрутизації в мережах передачі даних з урахуванням самоподібності трафіка / І.В. Гурман, В.В. Завадовський, І.В. Муляр //Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2014. – Вип. № 46. – С. 166-170.

4. Козак І.В Аналіз проблем захисту інформації в середовищі хмарних обчислень / І.В. Козак, С.О. Пашков, О.В. Огнєвий // Збірник наукових праць Військового інституту Київського національного

університету імені Тараса Шевченка. – К.: ВІКНУ, 2016. – Вип. № 51. – С.177–185.

5. Олифер, В.Г. Компьютерные сети / В.Г. Олифер. – СПб.: Изд– во Питер, 2004. – С. 198-199 .

6. Гладких А.А. Концептуальная модель функционирования обманной системы в условиях информационного противоборства. / А. А. Гладких, Р.Р. Зелимов // Сборник рефератов депонированных.– М: ЦВНИ МО РФ, 2004. - С. 12-15.

7. Моляков, А.С. Новые методы систематического поиска недекларированных возможностей ядра Windows NT 5. с введением контроля ContextHooking и PspCidHooking /А.С. Моляков // Вопросы защиты информации.– М.: Изд-во ВИМИ , 2008. – №1. – С. 39 - 45.

8. Муляр І.В. Розробка математичної моделі та методу її вирішення для підвищення ефективності використання обчислювальних ресурсів на основі технології віртуаліз / І.В. Муляр, Г.В. Гусляков, Л.В. Солодєєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2016. – Вип. № 54. – С. 134-143.

9. Козак І.В. Метод протидії прихованим загрозам в середовищі хмарних обчислень / І.В. Козак, О.В. Огнєвий // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2016. – Вип. № 54. – С.107-114

10. Муляр І.В. Аналіз прихованих загроз інформаційній безпеці у середовищі хмарних обчислень / І.В. Гурман, І.В. Муляр, Т.В. Бондаренко // Молодіжна військова наука у Київському національному університеті імені Тараса Шевченка : Всеукр. наук.-практ. конф. молодих вчених, ад'юнктів, слухачів, курсантів і студентів, 28 квіт. 2017 р.: тези доп. – К. : ВІКНУ, 2017. – С. 80.

11. Муляр І.В. Метод предикативної ідентифікації процесів для захисту від прихованих загроз в середовищі хмарних обчислень / С.В. Лєнков, В.М. Джулій, О.В. Селюков, І.В. Муляр // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2017. – Вип. № 55. – С. 145-154.

12. Ленков С.В. Динамічні показники оцінки рівня функціональної безпеки інформаційної системи / С.В. Лєнков, В.М. Джулій, І.В. Муляр // Сучасна спеціальна техніка. Науково практичний журнал. – ДНДІ МВС України, 2016. – Вип. №2(45). – С.59-67.

REFERENCES:

1. Muliar I.V. Analiz problem zabezpechennia funktsionalnoi bezpeky informatsiinykh system obrobky danykh / I.V. Muliar, A.V. Dzhulii, M.V. Kostiuk // Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh: Mizhnarodnyi naukovo-tekhnichnyi zhurnal. – Khmelnytskyi, 2013. – №1. – Pp. 133-138.

2. Moliakov, A.S. KPROCESSOR_CID_TABLE faktorynh – novii metod v teoryy kompiuternoho analyza vyrusnoho koda y poyska prohrammnыkh zakladok / A.S. Moliakov // Problemi ynformatsyonnoi bezopasnosty. Kompiuternыe systemi. - SPb.: Yzd-vo Polytekh. Un-ta, 2009. - №1. - c. 17-19.

3. Hurman I.V. Metod adaptyvnoi marshrutyzatsii v merezhakh peredachi danykh z urakhuvanniam samopodibnosti trafika / I.V. Hurman, V.V. Zavadovskyi, I.V. Muliar //Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU, 2014. – Vyp. № 46. – S. 166-170.

4. Kozak I.V Analiz problem zakhystu informatsii v seredovyshchi khmarnykh obchyslen I.V. Kozak, S.O. Pashkov, O.V. Ohnievyi // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU, 2016. – Vyp. № 51. – C.177-185

5. Olyfer, V.H. Kompiuternыe sety / V.H. Olyfer. - SPb.: Yzd- vo Pyter, 2004. – c. 198-199 .

6. Hladkykh A.A. Kontseptualnaia model funktsyonyrovanyia obmannoi systemы v uslovyiakh ynformatsyonnoho protyvoborstva. / A. A. Hladkykh, R.R. Zelymov // Sbornyk referatov deponyrovannыkh. - M: TsVNY MO RF, 2004. - c. 12-15.

7. Moliakov, A.S. Novie metodi systematycheskoho poyska nedeklaryrovannыkh vozmozhnostei yadra Windows NT 5. s vvedenyem kontrolia ContextHooking y PspCidHooking/ A.S. Moliakov // Voprosы zashchyty ynformatsyy. - M.: Yzd-vo VYMY, 2008. - №1. - c. 39 - 45.

8. Muliar I.V. Rozrobka matematychnoi modeli ta metodu yii vyrishennia dlia pidvyshchennia efektyvnosti vykorystannia obchysliuvalnykh resursiv na osnovi tekhnolohii virtualiz / I.V. Muliar, H.V. Husliakov, L.V. Solodieieva // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU, 2016. – Vyp. № 54. – C. 134-143.

9. Kozak I.V. Metod protydii prykhovanym zahrozam v seredovyshchi khmarnykh obchyslen / I.V. Kozak, O.V. Ohnievyi // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU, 2016. – Vyp. № 54. – C.107-114.

10. Muliar I.V. Analiz prykhovanykh zahroz informatsiinii bezpetsi u seredovyshchi khmarnykh obchyslen / I.V. Hurman, I.V. Muliar, T.V. Bondarenko // Molodizhna viiskova nauka u Kyivskomu natsionalnomu universyteti imeni Tarasa Shevchenka: Vseukr. nauk. -prakt. konf. molodykh vchenykh, ad'iunktiv, slukhachiv, kursantiv i studentiv, 28 kvit. 2017 r.: tezy dop. – K.: VIKNU, 2017. – S. 80.

11. Muliar I.V. Metod predykatyvnoi identyfikatsii protsesiv dlia zakhystu vid prykhovanykh zahroz v seredovyshchi khmarnykh obchyslen / S.V. Lienkov, V.M. Dzhulii, O.V. Seliukov, I.V. Muliar // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU, 2017. – Vyp. № 55. – C. 145-154.

12. Lenkov S.V. Dynamichni pokaznyky otsinky rivnia funktsionalnoi bezpeky informatsiinoi systemy / S.V. Lienkov, V.M. Dzhulii, I.V. Muliar // Suchasna spetsialna tekhnika. Naukovo praktychnyi zhurnal. - DNDI MVS Ukrainy, 2016. - Vyp. №2(45). - C.59-67.

Рецензент: д.т.н., проф. Лєнков С.В., головний науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка

к.т.н., доц. Муляр И.В., к.т.н., с.н.с. Мирошниченко О.В.,
к.т.н., с.н.с. Красник А.В., Солодеева Л.В.

ЗАЩИТА ОТ СКРЫТЫХ УГРОЗ В СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Наличие гипервизора в среде облачных вычислений создает новый класс угроз, реализация которых связана с неоднозначностью переходов между различными уровнями иерархии.

Применение современных технологий адаптивных систем защиты информации не позволяет осуществлять полный контроль за информационными потоками среды облачных вычислений, поскольку они функционируют на верхних уровнях иерархии. Поэтому для создания эффективных механизмов защиты ПО в среде облачных вычислений требуется разработка новых моделей угроз и создания методов отображения компьютерных атак, которые позволяют оперативно идентифицировать скрытые и потенциально опасные процессы информационного взаимодействия.

Автором разработана модель скрытых угроз информационной безопасности в среде облачных вычислений, учитывающий активный характер субъектов и объектов информационного взаимодействия.

Также разработана модель операций, происходящих с данными при их обработке в среде облачных вычислений, позволяет формализовать описание информационных процессов в виде мультиграфом транзакций.

Суть предлагаемого подхода заключается в представлении скрытой угрозы в виде функции предикатов, переменные которой явно инициализируются. Функция предикатов решаема для всех наборов переменных. Решение задачи противодействия скрытым угрозам формализуется с использованием набора предикатов, что позволяет представить функции оценки допустимости переходов в мультиграфе транзакций в виде набора таблиц правил политики безопасности.

Правила разграничения доступа, составляют основу политики безопасности, и включают ограничения на механизмы инициализации процессов доступа. В рамках разработаной модели операций формализованное описание скрытых угроз сводится к появлению контекстно-зависимых переходов в мультиграфе транзакций.

Ключевые слова:, гипервизор, облачные вычисления , кибербезопасность, скрытые угрозы.

Ph.D. Mulyar I.V., Ph.D. Miroshnichenko O.V., Ph.D. Krasnik A.V., Solodeeva L.V.

PROTECTION FROM HIDDEN THREATS IN THE CLOUD COMPUTING ENVIRONMENT

The presence of hypervisors in the cloud computing environment creates a new class of threats, the implementation of which is associated with ambiguity of transitions between different levels of the hierarchy.

Application of modern technologies of adaptive information security systems does not allow full control over the information flows of the cloud computing environment, since they function at the upper levels of the hierarchy. Therefore, to create effective mechanisms for protecting software in a cloud computing environment, it is necessary to develop new threat models and to create methods for displaying

computer attacks that allow operatively to identify hidden and potentially dangerous processes of information interaction.

The author developed a model of hidden threats to information security in the cloud computing environment, which takes into account the active nature of subjects and objects of information interaction.

Also developed a model of operations that occur with the data when processed in a cloud computing environment, which allows formalizing the description of information processes in the form of multi-transaction transactions.

The essence of the approach is to represent the hidden dangers in the form of a predicate function, which explicitly initialized variables. The predicate function is solved for all sets of variables. The solution to the problem of countering the hidden threats is formalized using the set of predicates that allows us to represent functions to assess the permissibility of transitions in the multigraph transaction in the form of a set of tables of rules of security policy.

Rules of access form the basis of security policy and include restrictions on the mechanisms of initialization processes access. Under the developed operations model, the formalized description of hidden threats is reduced to the emergence of context-dependent transitions in the multigraph transactions.

Keywords: the hypervisor, cloud computing, cybersecurity, hidden threats.