УДК 004.891

д.т.н., проф. **Лєнков С.В.** (ВІКНУ)
к.т.н., доц. **Джулій В.М.** (ХмНУ)
д.т.н., с.н.с. **Селюков О.В.** (ТОВ «Укрспецконсалтинг»)
к.т.н., доц. **Муляр І.В.** (ХмНУ)

МЕТОД ПРЕДИКАТИВНОЇ ІДЕНТИФІКАЦІЇ ПРОЦЕСІВ ДЛЯ ЗАХИСТУ ВІД ПРИХОВАНИХ ЗАГРОЗ В СЕРЕДОВИЩІ ХМАРНИХ ОБЧИСЛЕНЬ

У результаті досліджень, проведених авторами та оцінки впливу нових загроз на стан захищеності ресурсів середовищ хмарних обчислень випливає, що використання традиційних підходів не дозволяє вирішити проблему підвищення рівня захищеності середовища хмарних обчислень з урахуванням гнучкості, масштабованості (підтримки апаратних платформ різного класу) пропонованих програмно-технічних рішень мінімізації витрат. 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.

Відповідно, виникає необхідність в розробці 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.

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

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: хмарні обчислення, кібербезпека, приховані загрози, гіпервізор.

Вступ. Хмарні системи забезпечують просту й уніфіковану взаємодію між постачальником і користувачем включають програмне забезпечення, тобто сервісну підсистему, та базу даних із багаторазовим доступом. Хмарний сервіс є особливою клієнт-серверною технологією, яка передбачає використання клієнтом ресурсів (процесорного часу, оперативної пам'яті, дискового простору, мережевих каналів, спеціалізованих контролерів, програмного забезпечення тощо) групи серверів у мережі, які взаємодіють наступним чином:

• для клієнта вся група виглядає як єдиний віртуальний сервер;

• клієнт може прозоро та гнучко змінювати обсяги споживання ресурсів у разі зміни своїх потреб.

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. Дані хмарні системи відносяться до типу «інфраструктура як сервіс», і для них характерна наявність гіпервізора для управління обчислювальними ресурсами, який розглядається як додаткове джерело вразливостей, список яких з кожним роком збільшується. Застосування технологій хмарних обчислень визначає необхідність розгляду

можливих способів дестабілізуючих дій, що приводять до порушення функціонування компонентів інформаційного середовища.

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. Розробники програмно-технічних засобів захисту керуються власними уявленнями про створення прототипу продукту, використовуючи традиційні шаблони реалізації механізмів безпеки, саме тому часто представлені на ринку системи захисту інформації володіють множиною загальновідомих вразливостей навіть в умовах застосування новітніх технологій. 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.

У умовах розвитку ринкової економіки фахівцями різних країнах все більша увага приділяється питанням розробки засобів захисту, що дозволяють протидіяти загрозам інформаційній безпеці з боку зловмисників, на основі єдиного концептуального підходу, що поєднує в собі переваги різних методів захисту інформації. Розвиток засобів, методів і форм автоматизації процесів обробки інформації і масове застосування персональних комп'ютерів, що обслуговуються непідготовленими в спеціальному відношенні користувачами, роблять інформаційний процес уразливим по ряду показників [1].

Причини, які обумовлюють виникнення вразливостей у середовищі хмарних обчислень, наступні:

- об'єм оброблюваної інформації постійно збільшується з урахуванням розширення інформаційного простору мереж загального і спеціального призначення;
- у сучасних обчислювальних комплексах використовуються програмно-технічні засоби, різні по своїй архітектурі, функціональним можливостям і цільовому призначення;
- доступ до ресурсів обчислювальних комплексів отримує все більше число користувачів, операторів у зв'язку із застосуванням Internet-технологій;
- за рахунок використання нових, таких, що не пройшли тривалу апробацію в різних соціальних структурах технологій збільшується вірогідність виникнення нових класів вразливостей;
- низький рівень комп'ютерної грамотностіі користувачів, недостатня кваліфікація системних адміністраторів;
- передача інформації з використанням Wi-Fi мереж безпровідного доступу, що значно спрощує для зловмисника процес несанкціонованого знімання інформації, поширюваної за межі контрольованої зони.

Розвиток хмарних обчислень формує нові джерела загроз, які необхідно враховувати при забезпеченні захисту сучасних комп'ютерних систем і сервісів. Традиційні засоби захисту інформації контролюють тільки ті інформаційні потоки, які проходять по каналах, призначених для їх передачі, тому загрози, що реалізовуються за допомогою прихованих каналів передачі інформації, з їх допомогою не можуть бути виявленні та блоковані [2].

Постановка задачі. На основі попереднього аналізу виявлено, що зниження рівня захищеності обчислювальних систем пояснюється тією обставиною, що на сучасному етапі всього більшого поширення набувають атаки з використанням «руткітів», реалізуючих

технології DKOM і VICE, що дозволяють зловмисникам у вбудовуватися в керуючі операційні системи і безпосередньо здійснювати взаємодію з об'єктами ядра.

«Руткіти» даного класу функціонують на нижчому рівні, ніж модулі сучасних засобів захисту інформації, що вельми затруднює виявлення шкідливого коду. Надалі будуть розглянута модель операцій і модель прихованих загроз інформаційній безпеці по відношенню до середовища хмарних обчислень, що реалізовуються зловмисником за допомогою використання новітніх «руткіт»-технологій. При цьому необхідно звернути особливу увагу на рівні протоколів взаємодії різних модулів ОС, і розглянути механізми прихованого спостереження за процесами операційних систем, що реалізовують принципи «невидимості» для шкідливого коду, оскільки з найбільшою вірогідністю атака на комп'ютерну систему відбувається саме на цих рівнях [2].

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.

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.

Подальшу розробку нових технологій необхідно здійснювати на рівні протоколів взаємодії ОС і драйверів пристроїв, оскільки програмні модулі на вказаних інтерфейсних рівнях володіють привілейованими повноваженнями і можуть здійснювати довільні дії в операційних системах [3].

Однією з проблем, які потребують подальшого детального аналізу та вирішення, є проблема привілегійованих користувачів. Найбільшу загрозу для безпеки інформації в хмарі становлять користувачі, які мають привілейований доступ до функцій системи або адміністратори хмарних сервісів, тому для зменшення ризику можливих деструктивних дій з їх боку, доцільно вести незалежний нагляд та контроль за їх діями в хмарі.

Виклад основного матеріалу. Основою побудови хмарних сервісів є гіпервізор. Під гіпервізором зазвичай розуміють програму або апаратну схему, що забезпечує одночасне виконання декількох операційних систем на одному сервері віртуалізації. Гіпервізор дозволяє ізолювати різні ОС одна від одної.

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 $t > \mathrm{t0}$, 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.

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:

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

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 [2].

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

Необхідною умовою для вирішуваного завдання протидії прихованим загрозам є можливість спостереження переходів станів в мультиграфі транзакції.

Успішне вирішення завдання протидії прихованим загрозам математично припускає їх представлення у вигляді набору простих предикатів. При цьому функція оцінки допустимості переходів повинна бути описана у формі кон'юнкції простих предикатів.

На основі комбінаторного аналізу можливих переходів при виникненні подій з множини E необхідно довести, що при числі рівнів ієрархії рівним 8 відображення $Si\ x\ Ei :\to Sj$. 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 $n!$.

Процес може існувати на m - рівнях ієрархії. У нашому випадку число предикатів рівне 3. Розмірність таблиці інцидетності -$12x4 = 48$. Тоді умову ізоморфності можна записати у вигляді $3!*m = 48$. Звідси витікає, що $m = 8$. При $m < 8$ відображення не ізоморфно.

Кожен компонент гіпервізора описується кінцевим автоматом

$$\mathrm{mod}_i = (Ei, Ri, start, \Pr ivi, Fi, Pi, Vi), \quad (1)$$

де $\mathrm{mod}_i \in M$ – 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

$$Pi = (s, Ord, Context\_type). \quad (2)$$

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

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. В результаті будь-який ініціатор процесу доступу може використовувати тільки дозволені послідовності операцій, ознака яких задається кортежем предикатів $(s, Ord, Context\_type)$.

На рис.1 приведений приклад перехоплення системного виклику гостьової ОС на рівні гіпервізора

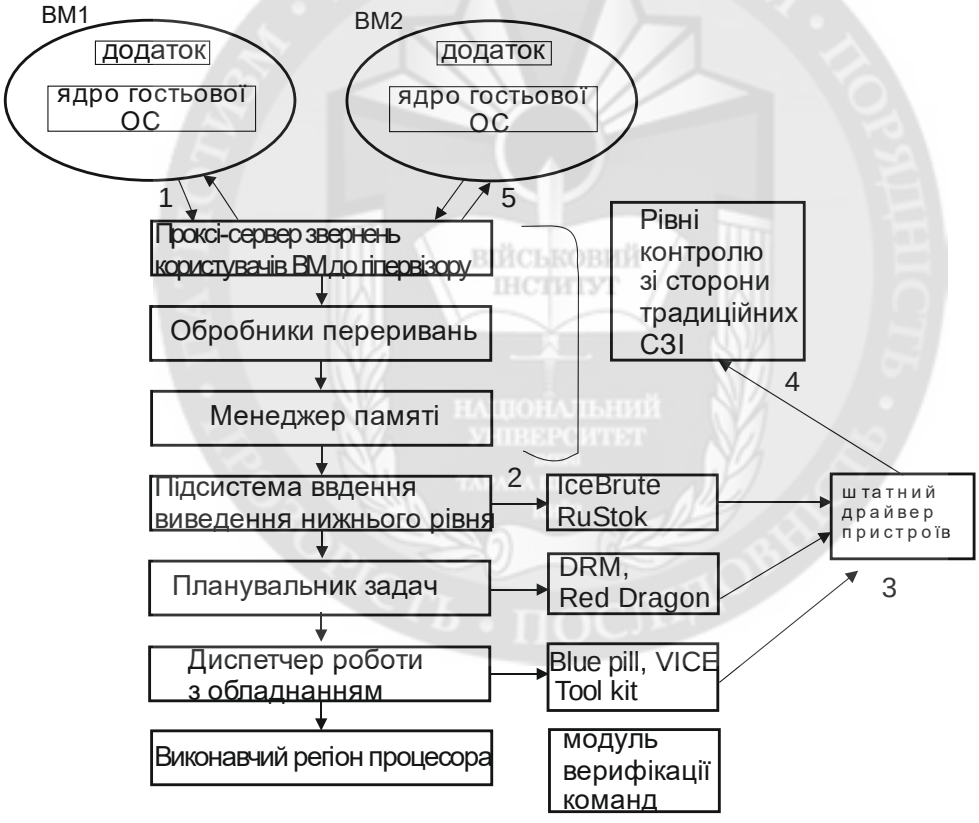

Рис. 1. Приклад перехоплення системного виклику гостьовою ОС на рівні гіпервізора

Зовнішніми діями Vi є запити користувачів ВМ, що поступають на обробку гіпервізора, або процеси шкідливого ПЗ, модифікуючі компоненти гіпервізора.

Оскільки носієм станів гіпервізора hv, що входить в, є множина подій E, яка складається з двох непересічних підмножин: Ehv - множина подій, що виникають на рівні

гіпервізора, множина Evm – множина подій, що генеруються віртуальними машинами vm, зокрема запити користувачів на зміну сценаріїв конфігурацій ВМ $\{conf\}$, то порушник може використовувати для атаки множину подій, що генеруються віртуальними машинами за допомогою «вбудовування» шкідливих операцій на нижні рівні ієрархії середовища виконання команд ВМ, які не контролюються традиційними СЗІ, але реалізуються за допомогою каналів міжпроцесного обміну, що змінює контекст виконання операцій.

Така дія може змінювати послідовність переходів з одного функціонального рівня моделі гіпервізора на інший.

На рис. 1 приведений приклад перехоплення системного виклику гостьових ОС на рівні гіпервізора з урахуванням можливості виникнення прихованих загроз безпеки і для інформаційних ресурсів віртуальних машин ВМ1 і ВМ2.

Зважаючи на структуру взаємодії системних і прикладних процесів (див. рис. 2.3.1), за допомогою мультиграфа транзакцій $G =< R,\ D,\ I >$ можна описати переходи між всіма станами гіпервізора. При цьому стани $Ri = \{R1, R2, R3, R4, R5, R6, R7, R8\}$ представляються вершинами графа; Di – ребра, що представляють можливі переходи між станами Ri ; Ij - матриця інциденцій мультиграфа. Лівими стрілками $p1, p2, p3, p4, p5, p6, p7$ позначені переходи в мультиграфі транзакцій без зміни контексту виконання операцій. Правими стрілками $q1, q2, q3, q4, q5, q6, q7$ позначені переходи із зміною контексту виконання операцій, коли компонент $\mathrm{mod}\, i$ модифікований шкідливим ПЗ. Як видно з рис. 1 компоненти гіпервізора можуть модифікуватися шкідливим ПЗ в результаті успішних атак внутрішнього порушника ВМ. Крім того, гіпервізор не є довіреним і представляє джерело загроз по причині того, що часто застосовуються гіпервізори, не сертифіковані по вимогах безпеки.

Стрілками 1 позначено проходження запиту від ВМ1 до гіпервізора, стрілками 5 – проходження запиту від ВМ2 до гіпервізора. Стрілками 3 показані канали перехоплення даних модулями шкідливого ПЗ, наприклад IceBrute, RuStock, DRM, Croax, Red Dragon, Blue Pill, VICE Toolkit, які модифікують дані, отримані від користувача ВМ1 (стрілки 2), і відправляють їх за допомогою використання штатного драйвера для роботи з пристроями (наприклад, диск, мережевий контролер і тому подібне) користувачеві ВМ2 (стрілка 4).

Набір міток *{m}* для «розфарбовування» мультиграфа є значеннями предикатів $(s, Ord, Context\_type)$. Зміна контексту виконання запиту формалізується у вигляді матриці інцидентності гіпервізора.

Істотною особливістю даних операцій, є те, що суб'єкти і об'єкти доступу можуть мінятися ролями. Тому для контролю незмінності об'єктів пропонується використовувати монітор безпеки, який реалізує спеціальні механізми ідентифікації контексту контрольованих потоків даних, як для суб'єктів, так і для об'єктів доступу, при цьому ініціатор доступу може використовувати тільки дозволені послідовності операцій у вигляді кортежу $(s, Ord, Context\_type)$. $Context\_id$ – ідентифікатор запиту, що виконується користувачем ВМ

Таблиця 1

Матриці інцидентності мультиграфа транзакцій розміром 12x4.

Біт S	Ord	Context_type	Context_id
	0	0	*Context_id1*
1	1	0	*Context_id2*

Біт S	Ord	Context_type	Context_id
0	1	0	*Context_id3*
1	0	0	*Context_id4*
0	0	1	*Context_id5*
0	0	-1	*Context_id6*
0	1	1	*Context_id7*
0	1	-1	*Context_id8*
1	0	1	*Context_id9*
1	0	-1	*Context_id10*
1	1	1	*Context_id11*
1	1	-1	*Context_id12*

Кількість рядків в таблиці інциденцій мультиграфа транзакцій дорівнює 12 тому, що для опису контекстно-залежних переходів використовується кортеж з трьох предикатів $s, Ord, Context\_type$, при цьому кожна змінна може приймати два значення: 0 і 1. Тоді загальне число комбінацій дорівнює 3!2!= 12 .

Подібно до системних викликів, за допомогою яких створюється місток між додатками і функціями ядра ОС, інтерфейс гіпервикликів забезпечує надходження запитів з ВМ в гіпервізор. Підсистему введення/виводу нижнього рівня можна віртуалізувати в ядрі, або в гостьову систему потрібно додати код доступу до введення/виводу. Переривання повинні оброблятися тільки гіпервізором, який має справу з реальними перериваннями і здійснюватиме передачу переривань віртуальних пристроїв в операційну систему ВМ.

Гіпервізор повинен відловлювати і обробляти виняткові стани, які виникають в гостьовій системі.

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 ініціалізуются. 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 розробленної 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, 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.

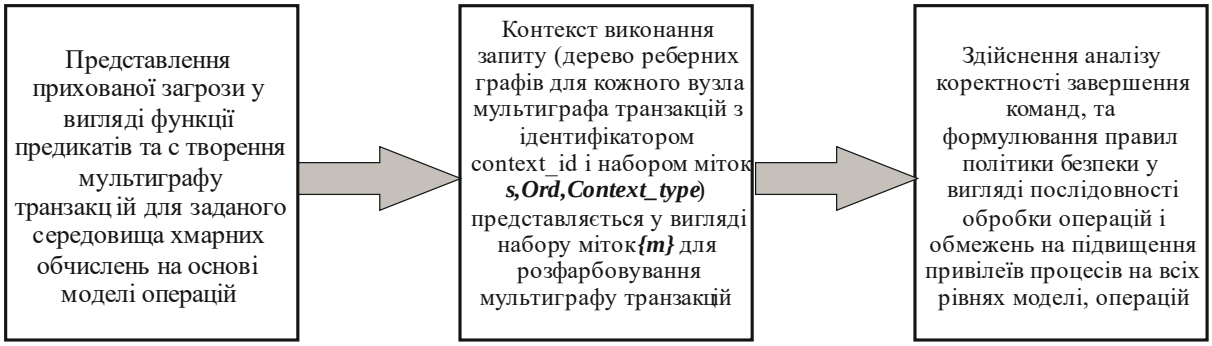

Рис. 2. Графічне представлення методу предикативної ідентифікації процесів для захисту від прихованих загроз

Послідовність кроків для реалізації пропонованого підходу наступна:

1. Спочатку створюється мультиграф транзакцій для заданого середовища хмарних обчислень на основі запропонованої моделі операцій.
2. Контекст виконання запиту представляється у вигляді набору міток *{m}*.
3. Здійснюється аналіз коректності завершення команд. В результаті правила вибраної політики безпеки формулюються в термінах, які задають послідовність обробки операцій і обмежень на підвищення привілеїв процесів на всіх рівнях моделі, представленої на рис. 2.

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 (таблиця 2).

Таблиця 2

Таблиця правил ПБ

Поле *s*	Поле *Ord*	Поле *Context_type*	Таблиця правил політики безпеки
0	*X*	-1	*False* - заборонити, оскільки здійснюється спроба пошкодити компоненти гіпервізора з боку зловмисника за рахунок перехоплення звернень користувачів ВМ до драйверів пристроїв
0	*X*	1	*False* - заборонити, оскільки здійснюється спроба зловмисника змінити дані про конфігурацію ВМ
1	*X*	*X*	*True* – дозволити стани
0	0	0	Очікування запитів користувачів і їх реєстрація

На основі заданих таблиць правив ПБ контролюється активність мережевих додатків, звернень до пристроїв ВМ і відстежуються вхідні і вихідні пакети даних.

Висновки. Існують неявні механізми несанкціонованого підвищення повноважень доступу до об'єктів гостьової ОС, що обумовлює необхідність розробки нових методів і алгоритмів, що дозволяють «прозоро» управляти інформаційними потоками 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.

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. 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

3. 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.

REFERENCES:

1. Mulyar I.V. Analiz problem zabezpechennya funktsional'noyi bezpeky informatsiynykh system obrobky danykh /I.V. Mulyar, A.V. Dzhuliy, M.V. Kostyuk // // Vymiryuval'na ta obchyslyuval'na tekhnika v tekhnolohichnykh protsesakh: Mizhnarodnyy naukovo-tekhnichnyy zhurnal.-Khmel'nyts'kyy, 2013.-#1 -S. 133-138.

2. Kozak I.V. Metod proty`diyi pry`xovany`m zagrozam v seredovy`shhi xmarny`x obchy`slen` / I.V. Kozak, O.V. Ognyevy`j // Zbirny`k naukovy`x pracz` Vijs`kovogo insty`tutu Ky`yivs`kogo nacional`nogo universy`tetu imeni Tarasa Shevchenka. – K.: VIKNU, 2016. – Vy`p. # 54. – C.107-114

3. Molyakov, A.S. KPROCESSOR_CID_TABLE faktoring – novyiy metod v teorii kompyuternogo analiza virusnogo koda i poiska programmnyih zakladok/ A.S. Molyakov // Problemyi informatsionnoy bezopasnosti. Kompyuternyie sistemyi. - SPb.: Izd-vo Politeh. Un-ta, 2009. - #1. - c. 17-19.

д.т.н., проф. Ленков С.В., к.т.н., доц. Джулий В.Н.,
д.т.н. с.н.с. Селюков А.В., к.т.н., доц. Муляр И.В.

МЕТОД ПРЕДИКАТИВНОЙ ИДЕНТИФИКАЦИИ ПРОЦЕССОВ ДЛЯ ЗАЩИТЫ ОТ СКРЫТЫХ УГРОЗ В СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

В результате исследований, проведенных авторами и оценки влияния новых угроз на состояние защищенности ресурсов среды облачных вычислений следует, что использование традиционных подходов не позволяет решить проблему повышения уровня защищенности среды облачных вычислений с учетом гибкости, масштабируемости (поддержки аппаратных платформ различного класса) предлагаемых программно-технических решений минимизации затрат. Поэтому для создания эффективных механизмов защиты ПО в среде облачных вычислений нужна разработка новых моделей угроз и создание методов отражения

компьютерных атак, которые позволяют оперативно идентифицировать скрытые и потенциально опасные процессы информационного взаимодействия. Соответственно, возникает необходимость в разработке новых средств защиты информации, основанных на методах оперативной идентификации потенциальных уязвимостей, возникающих как на уровне процессов контроля доступа к ресурсам гостевых ОС, так и на уровне системных вызовов гипервизора, которые при определенных условиях сами могут становиться источниками различных видов разрушающих воздействий. Наличие гипервизоров в среде облачных вычислений создает новый класс угроз, реализация которых связана с неоднозначностью переходов между различными уровнями иерархии.

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: облачные вычисления, кибербезопасность, скрытые угрозы, гипервизор.

Prof. Lenkov S.V., Ph.D. Dzhuliy V.M., prof. Selyukov A.V., Ph.D. Muliar I.V.

METHOD OF THE PROCESSES PREDICTIVE IDENTIFICATION FOR PROTECTION OF HIDDEN THREATS IN CLOUD COMPUTING ENVIRONMENT

As a result of research conducted by the authors, and assess the impact of new threats to the security of the state of the resources of cloud computing environment, it is possible to make conclusion that the use of traditional approaches cannot solve the problem of increasing the level of cloud computing environment security with flexibility, scalability (hardware platforms support different class) offers software and hardware solutions to minimize costs. Therefore, to create effective mechanisms for protecting software in a cloud computing environment we need the development of new threat models and the creation of reflection methods of computer attacks which allow us to identify hidden and potentially dangerous processes of information interaction.

Accordingly, there is a need to develop new means of information protection, based on methods for the rapid identification of potential vulnerabilities occurring at the level of access control processes to the guest operating system resources, and at the level of the system calls the hypervisor, which under certain conditions can themselves become sources of different kinds of destructive effects. The presence of a hypervisor in the cloud computing environment creates a new class of threats, the implementation of which is associated with the ambiguity of transitions between different hierarchy levels.

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