УДК 004.891

**Козак І.В.** (ХмНУ)
к.т.н., доц. **Огнєвий О.В.** (ХмНУ)

# МЕТОД ПРОТИДІЇ ПРИХОВАНИМ ЗАГРОЗАМ В СЕРЕДОВИЩІ ХМАРНИХ ОБЧИСЛЕНЬ

***У результаті проведеного аналізу в статті доводиться актуальність розробки технології протидії спробам змінити стан захищеності інформаційних ресурсів у середовищі хмарних обчислень. В результаті досліджень, проведених авторами, зроблено висновок про те, що перспективним напрямком вдосконалення технологій кіберзахисту в середовищі хмарних обчислень є розробка методів протидії загрозам, які реалізуються з допомогою процесів, в яких суб'єкти і об'єкти інформаційної взаємодії можуть використовувати різні канали передачі даних, у тому числі і приховані. Показано, як реалізація прихованих загроз дозволяє шкідливому коду маскуватися під системний процес, завдаючи шкоди безпеці середовища хмарних обчислень за допомогою блокування, розкрадання, знищення або несанкціонованої передачі інформації.***

***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.***

***Відповідно, виникає необхідність в розробці математичної моделі прихованих загроз інформаційної безпеки, в якій враховується поведінковий характер об'єктів інформаційної взаємодії. Також розроблено модель інформаційного забезпечення для хмарних обчисленнях, що дозволяє представити формалізований опис інформаційних процесів у середовищі хмарних обчислень у вигляді мультиграфа транзакцій. На основі цих моделей розроблено метод протидії прихованим загрозам, заснований на контролі транзакцій, що відповідають вимогам політики безпеки.***

***Ключові слова: кібербезпека, хмарні обчислення, приховані загрози, захист інформації.***

**Вступ**. Доктрина інформаційної безпеки України визначає поняття інформаційної сфери як сукупність інформації, інформаційної інфраструктури, суб'єктів, що здійснюють збір, формування, розповсюдження і користування інформації, а також системи регулювання суспільних відносин, що виникають при цьому. Інформаційна безпека в широкому сенсі є таким станом об'єкту захисту, яке, виключає можливість нанесення шкоди властивостям об'єкту, обумовленою його взаємодією з інформаційною сферою [1]. Згідно стандартів загроза безпеці визначається як сукупність умов і чинників, що створюють потенційну або таку, що реально існує небезпеку, пов'язану з просочуванням інформації і/або несанкціонованими і/або ненавмисними діями на неї.

Стрімкий розвиток технологій віртуалізації і створення середовищ хмарних обчислень формує нові джерела загроз, які необхідно враховувати при забезпеченні кібербезпеки сучасних комп'ютерних систем і сервісів. При цьому динамічний характер процесів інформаційної взаємодії істотно ускладнює можливості оперативної оцінки ризиків порушення конфіденційності, цілісності і доступності програмних та інфраструктурних ресурсів, що надаються в режимі віддаленого доступу.

Традиційні засоби забезпечення інформаційної безпеки такі, як засоби розмежування доступу, міжмережеві екрани, системи виявлення вторгнень, контролюють тільки ті інформаційні потоки, які проходять по каналах, призначеним для їх передачі, тому загрози, які реалізуються за допомогою прихованих каналів передачі інформації, з їх допомогою не можуть бути блоковані. В цих умовах важливого значення набувають технології захисту від загроз, які формуються з використанням прихованих каналів інформаційного впливу або всередині периметра безпеки корпоративної комп'ютерної мережі. Захист від таких деструктивних впливів повинна здійснюватися на рівні процесів управління системними викликами або контролю недекларованих можливостей прикладного програмного забезпечення, що вимагає створення нових моделей і методів протидії спробам як зовнішніх,

так і внутрішніх користувачів змінити стан захищеності інформаційних ресурсів середовища хмарних обчислень.

Хмарні технології стануть основою для формування нового простору, що створюється в рамках ініціативи, що отримала назву Intelligence Community Information Technology Enterprise.

У роботі по розгортанню хмарної платформи беруть участь фахівці всього розвідувального співтовариства США, яких припадає на частку основна частина бюджету американської розвідки [2].

Наприклад, ЦРУ розробляє захищену хмарну обчислювальне середовище для всього розвідувального співтовариства.

Ідея, що лежить в основі розвитку і впровадження розподілених інформаційних технологій хмарних обчислень в розвідувальну діяльність, давно стала стійким трендом для багатьох федеральних відомств і комерційного сектора США і привела до істотного скорочення їх трудовитрат. При цьому користувачі будуть усунені від технічних деталей, таких як операційна система, інфраструктура і програмне забезпечення. Все це користувачам надається за допомогою хмарного сервісу. Міністерство оборони США вийшло з ініціативою підключити до нього не тільки свої відомства, але і промисловість, а також інші урядові установи. Вже до 2016–2020 років у формований простір повинні інтегруватися численні розрізнені хмарні платформи Міністерства оборони США, розвідувального співтовариства, військово-промислового комплексу, уряди і інші організації.

**Постановка задачі**. Важливим напрямком вдосконалення технологій захисту та систем інформаційної безпеки є протидія білатеральним загрозам, у яких суб'єкт та об'єкт процесів інформаційної взаємодії є потенційним носієм небезпечних впливів. У таких випадках необхідно використовувати моделі загроз, які ідентифікують потенційні уразливості 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 руйнівних впливів, 6 реалізуються шляхом порушення функціонування планувальника завдань або диспетчера обладнання. Виникаючі при цьому загрози необхідно не тільки оперативно виявляти, але і блокувати використовуються неавторизовані канали інформаційних впливів, які у середовищі хмарних обчислень зазвичай реалізуються в прихованому для гостьових ОС режимах [3.

Хмарні системи класу «інфраструктура як сервіс» можуть стати джерелом загроз порушення безпеки програмного забезпечення, що пов'язано з активним характером взаємодії суб'єктів і об'єктів доступу до інформаційних ресурсів і призводить до ризиків порушення цілісності та доступності програмних сервісів, що надаються в режимі віддаленого доступу. Особливу небезпеку надають загрози, які реалізуються всередині периметра безпеки комп'ютерної мережі, так як їх локалізація із застосуванням сучасних засобів захисту інформації [3].

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.

Відповідно, виникає необхідність в розробці математичної моделі прихованих загроз інформаційної безпеки, в якій враховується поведінковий характер об'єктів інформаційної взаємодії.

**Виклад основного матеріалу.** На основі попереднього аналізу 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.

Для середовища хмарних обчислень однією з головних проблем управління є нерівномірність запиту ресурсів з боку клієнтів. Для згладжування нерівномірності надання сервісів, т.д. розподілу ресурсів між реальним апаратним забезпеченням і хмарним програмним забезпеченням, використовують проміжний шар серверної віртуалізації.

Захист самих віртуальних машин. На відміну від фізичної машини, коли віртуальна машина вимкнена, залишається можливість її компрометації або «зараження». Тим же, хто використовує сервіси хмарних обчислень, слід переконатися в тому, що провайдер має системи захисту інформації, які встановлені на серверах віртуалізації.

Одночасно проводиться оцінка небезпеки реалізації загрози, що визначається трьома параметрами:

- низька небезпека – якщо реалізація може призвести до загрози незначним негативних наслідків для суб'єктів персональних даних;
- середня небезпека – якщо реалізація може призвести до загрози негативних наслідків для суб'єктів персональних даних;
- висока небезпека – якщо реалізація може призвести до загрози значних негативних наслідків для суб'єктів персональних даних.

У середовищі хмарних обчислень головною умовою виступає повнофункціональна підтримка програмного забезпечення сторонніх виробників і можливість швидкого (гнучкого) налаштування окремих компонентів. Інформаційні системи даного класу на відміну від комунікаційних мереж спеціального призначення не можуть «існувати» в ізоляції з боку апаратно-програмних засобів контролю, забезпечення достовірності і захисту ПО. Слід зазначити важливу роль мереж в умовах глобалізації процесів навчань, розвитку Internet, технологій проведення відеоконференцій в режимі реального часу, розвитку партнерських науково-дослідних програм в рамках проектів ЮНЕСКО і ООН, співпраці комерційних і державних установ освітнього призначення.

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 .

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 забезепечення, встановленого на серверах віртуалізації Логіка виконання програм повинна контролюватися з точки зору відмови в обслуговуванні. Це підвищує ризики від реалізації прихованих погроз. не тільки функціональних можливостей, але і безпеки, яка оцінюється величиною ризику їх не документованої роботи. Для цього необхідно добре уявляти, що і як може загрожувати нормальному функціонуванню системи, що захищається. При цьому шкідливе прогамне забезпечення не здійснює блокування і знищення інформації, циркулюючої в системі, не перехоплює системні виклики гостьових ОС, а «вбудовується» безпосередньо на рівні планувальника завдань і диспетчера роботи з устаткуванням гіпервізора і може ушкоджувати програмному забезпеченні гіпервізора. Приховані погрози, 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.

Під реалізацією прихованих погроз 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.

Тому для протидії прихованим погрозам 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:

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

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.

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 погроз.

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

$$\langle\ Source, Services, Measuring, \{proc\}, Actions, \{hv\}, \{vm\}, Security\ Roles\ \rangle,$$

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

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

$Measuring$ - 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.);

$Actions$ $(дії)$ - множина суб'єктів впливу (шкідливий код гіпервізора, несертифіковані засоби віртуалізації і. т. п.); множина суб'єктів впливу (шкідливий код гіпервізора, несертифіковані засоби віртуалізації і. т. п.);

$\{hv\}$ - середовище ВМ у гіпервізорі, що представляє собою безліч 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 погроз 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 має на увазі та обставина, що вони можуть мінятися місцями. Розглянемо ситуацію, в якій зловмисник(суб'єкт) атакує сервер віртуалізації(об'єкт), модифікує компоненти гіпервізора шляхом реалізації нових погроз, 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 гіпервізору |
| Загроза порушення однозначності переходів станів при обміні інформацією між віртуальною машиною та гіпервізором | Можливість отримання несанкціонованого доступу до данних користувача іншої віртуальної машиши |
| Загроза модифікації програмного забезпечення гіпервізорі | Поширення шкідливого програмного забезпечення в середовищі хмарних обчислень |

При цьому «заражені» гіпервізори, що знаходяться в одній або різних підмережах, стають учасниками атаки, тобто суб'єктами доступу, а запущеними під їх управлінням віртуальні машини користувачів - об'єктами.

Середовище хмарних обчислень може бути представлене у вигляді 8 - рівневої ієрархічної моделі.

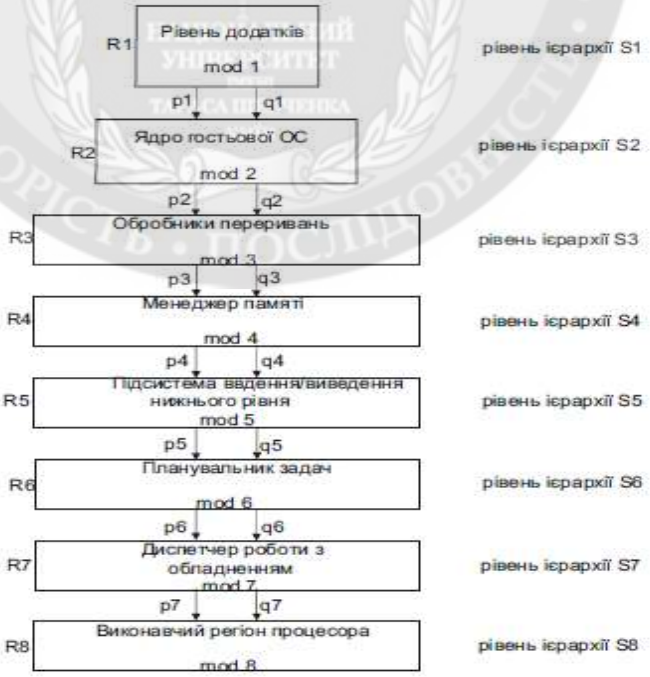


Рис. 1. Ієрархічна модель середовища хмарних обчислень

На рис. 1 використовуються такі позначення:

$R..R8$ – стан процесів; $S1$ – 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 обладнанням гіпервізора; $S8$ – рівень виконавчого процесора. На рівнях $S1-S5$ функціонують традиційні системи захисту інформації, які використовують набори правил контролю доступу, що відповідають вимогам політики безпеки. На рівнях $S6-S7$ реалізуються приховані для гостьових ОС загрози, а на рівні $S8$ здійснюється контроль виконання операцій. Лівими стрілками $p1-p7$ позначені переходи в мультиграфі транзакцій без зміни контексту виконання операцій. Правими $q1-q7$ позначені переходи зі зміною контексту виконання операцій, коли компонент $\mathrm{mod}\,i$ модифікований шкідливим програмним забезпеченням.

На основі запропонованої декомпозиції модель операцій можна конструктивно представити за допомогою мультиграфа транзакцій, який описує дозволені механізми ініціалізації процесів доступу до прикладних і системних інформаційних ресурсів. В результаті запропонованої формалізації опис прихованих загроз зводиться до введення контекстно-залежних переходів в мультиграфе транзакцій, тому для їх виявлення потрібно розробка ефективних алгоритмів ідентифікації стану як прикладних, так і системних процесів.

**Висновки.** Розроблена модель прихованих загроз, в якій враховується активний характер суб'єктів та об'єктів інформаційної взаємодії. Для формалізації опису даних процесів запропоновано модель операцій, виконуваних на різних рівнях функціонування середовища хмарних обчислень. В запропонованій моделі операцій різні компоненти гіпервізора розглядаються в якості потенційного джерела загроз інформаційній безпеці, які реалізується шляхом поширення шкідливого програмного забезпечення або ініціалізації процесів, що руйнують стан захищеності ресурсів середовища хмарних обчислень. За допомогою розробленої моделі запропоновано формалізований опис загроз, які формують послідовності запитів до некоректних програмним модулям гіпервізора або використовують недекларовані можливості системного і прикладного програмного забез.

Запропонований підхід до опису операцій заснований на класифікації ризиків порушення інформаційної безпеки та аналізі контексту виконання потоків команд, за допомогою яких можуть передаватися дані в обхід вимог прийнятої політики безпеки, що призводить до порушення захищеності ресурсів гіпервізора. В розробленій моделі носіями аналізованих операцій є множини об'єктів і суб'єктів доступу, яким присвоєно різні рівні безпеки.

ЛІТЕРАТУРА:

1. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №555/2015. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року "Про нову редакцію Воєнної доктрини України" [Електронний ресурс] / П.О. Порошенко.
- Режим доступу http://www.president.gov.ua/documents/5552015-19443.

2. 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.

3. 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.164-171

4. 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. UKAZ PREZYDENTA UKRAYiNY #555/2015Pro rishennya Rady natsional'noyi bezpeky i oborony Ukrayiny vid 2 veresnya 2015 roku "Pro novu redaktsiyu Voyennoyi doktryny Ukrayiny" [Elektronnyy resurs] / P.O. Poroshenko // Rezhym ostupu http://www.president.gov.ua/documents/5552015-19443

2. Kozak I.V. Analiz problem zakhystu informatsiyi v seredovyshchi khmarnykh obchyslen' / I.V. Kozak, S.O. Pashkov, O.V. Ohnyevyy // Zbirnyk naukovykh prats' Viys'kovoho instytutu Kyyivs'koho natsional'noho universytetu imeni Tarasa Shevchenka. – K.: VIKNU, 2016. – Vyp. # 51. – C.164-171

3 . 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.

4. 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.

**Рецензент: д.т.н., проф. Сбітнєв А.І.**

**Козак І.В., к.т.н., доц., Огнєвий О.В.**

## МЕТОД ПРОТИВОДЕЙСТВИЯ СКРЫТЫМ УГРОЗАМ В СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

***По результатам проведеного анализа в статье доказывается актуальность разработки технологии противодействия попыткам изменить состояние защищенности информационных ресурсов в среде облачных вычислений. В результате проведенных авторами исследований сделан вывод о том, что перспективным перспективным направлением совершенствования технологий киберзащиты в среде облачных вычислений является разработка методов противодействия угрозам, реализуемым с помощью процессов, в которых субъекты и объекты информационного взаимодействия могут использовать различные каналы передачи данных, в том числе и скрытые. Показано, как реализация скрытых угроз позволяет вредоносному коду маскироваться под системный процесс в ущерб безопасности среды облачных вычислений с помощью блокировки, хищения, уничтожения или несанкционированной передачи информации.***

***Для борьбы с такими угрозами актуальна разработка 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 разрушительных воздействий.***

***Соответственно, возникает необходимость в разработке математической модели скрытых угроз информационной безопасности, в которой учитывается поведенческий характер объектов информационного взаимодействия. Также разработано модель информационного обеспечения для облачных вычислений, что позволяет представить формализованное описание информационных процессов в среде облачных вычислений в виде мультиграфа транзакций. На основе этих моделей разработан метод противодействия скрытым угрозам, основанный на контроле транзакций, соответствующих требованиям политики безопасности.***

***Ключевые слова: кибербезопасность, облачные вычисления, скрытые угрозы, защита информации.***

**Kozak I.V., Ph.D. Ohnevyj A.V.**

# METHOD OF THE COUNTERACTING THE HIDDEN THREATS IN THE CLOUD COMPUTING ENVIRONMENT

***As a result of the analysis, the authors of this article prove the relevance of developing the counteracting technology to the attempts of changing the condition of protecting the information resources in the cloud computing environment. At the end of the research, authors made a conclusion that the promising direction of improving the cyberprotecting technology is to develop methods of counteracting the threats, which are realized through the processes in which subjects and objects of the information exchange may use different data transmission channels, including the hidden ones. Authors showed how the realization of hidden threats allows the harmful code to disguise as a systemic process, harming the security of the cloud computing environment with the help of blocking, theft, destruction or unauthorized transfer of information.***

***To fight such threats it is relevant to develop the new information security based on the methods of rapid identification of potential vulnerabilities arising at the level of processes of controlling the access to the resources of the guest OS and at the level of system hypervisor's calls, which under certain conditions can become sources of different types of destructive influence.***

***Consequently, there is a necessity to elaborate a mathematical model of hidden threats of the information security, which takes into account the behavioral nature of the information interaction of objects. Also the authors created the model of information support for cloud computing, which allows to introduce a formalized description of information processes in the cloud computing environment as a multigraph of transactions. On the basis of these models the researchers developed a method of counteracting the hidden threats, based on the control of transactions that meet the requirements of security policy.***

***Keywords: cybersecurity, cloud computing, hidden threats, protection of the information.***