УДК 004.891

Козак І.В. (ХмНУ)
к.військ.н., доц. **Пашков С.О.** (ВІКНУ)
к.т.н., доц. **Огнєвий О.В.** (ХмНУ)

АНАЛІЗ ПРОБЛЕМ ЗАХИСТУ ІНФОРМАЦІЇ В СЕРЕДОВИЩІ ХМАРНИХ ОБЧИСЛЕНЬ

У статті проведено аналіз існуючих загроз, що реалізуються з використанням прихованих каналів і декларованих можливостей програмного забезпечення (ПЗ). 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.

Особливу увагу приділено аналізу недоліків сучасних технологій захисту інформації в середовищі хмарних обчислень, які не враховують динамічний характер наданих прикладних і системних програмних сервісів.

Ключові слова: хмарні обчислення, кібербезпека, інформаційна безпека, приховані загрози, комп'ютерні системи.

Вступ. 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 (НДВ) прикладного програмного забезпечення (ПО), що вимагає створення нових моделей і методів протидії спробам як зовнішніх, так і внутрішніх користувачів змінити стан захищеності інформаційних ресурсів середовища хмарних обчислень.

Актуальність вирішення цієї важливої науково-технічної задачі відзначається багатьма зарубіжними вченими, у тому числі В. А. Курбатовым., П. Д. Зегждой, А. А. Грушо, Е. Е. Тимониной, В. Ю. Скибой, Н.А.Гайдамакиным, А. А. Гладких, В. С. Заборовським, С. Воглом, Р. Сэйлером, Ф. Мортинелли, Дж. Рутковській та ін. У роботах перелічених авторів велика увага приділяється розробці засобів захисту інформації, яких враховуються особливості технологій віртуалізації і можливості сучасних апаратно-програмних компонент обчислювальних систем, що безпосередньо впливають на захищеність системних і прикладних процесів. У зарубіжних наукових публікаціях описуються лише базові підходи контролю сигнальних подій у «контурі» розподілених обчислювальних систем. У сучасних наукових школах США та Великобританії (на підставі відкритих публікацій) дослідження вірусного коду і вивчення методів виявлення програмних «закладок» використовується класичний підхід – специфікація базових сервісів ОС, маркерні сигнатури, динамічний аналіз виконуваного коду на рівні KOS (Kernel Object Specification). Дані дослідження не зачіпають розгляд проблеми «неявних» механізмів контролю ресурсів операційної системи і принципів «невидимості». Класичні підходи та методи з використанням згаданої вище специфікації KOS не дозволяють виявляти нові зразки шкідливого ПЗ, що використовує технології DCOM (Direct Kernel Object Manipulation) і VICE(Virtual ICE).

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.

Постановка задачі. 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 (СЗІ).

Важливим фактором підвищення ефективності систем захисту від прихованих загроз є облік напрямку передачі, синтаксису і контексту переданих потоків даних. З урахуванням вищесказаного, захист від загроз, які можуть призводити до розкрадання даних, неконтрольованої модифікації програмних кодів, порушення доступності (блокування) або нав'язування хибної інформації в середовищі хмарних обчислень є актуальною науково-технічною задачею.

На основі проведеного аналізу та оцінки впливу нових загроз на стан захищеності ресурсів середовища хмарних обчислень метою даної роботи є :

1. Аналіз характерних особливостей сучасного середовища хмарних обчислень.
2. Аналіз сучасних підходів і технологій захисту інформаційних ресурсів середовища хмарних обчислень.
3. Виявлення недоліків сучасних технологій захисту інформації в середовищі хмарних обчислень.

Аналіз відомих досліджень і публікацій. Доктрина інформаційної безпеки визначає поняття інформаційної сфери як сукупність інформації, інформаційної інфраструктури, суб'єктів, що здійснюють збір, формування, розповсюдження та користування інформації, а також системи регулювання виникаючих при цьому громадських відносин. Інформаційна безпека в широкому розумінні являє собою такий стан об'єкта захисту, який виключає можливість нанесення шкоди властивостями об'єкта, обумовлена його взаємодією з інформаційної сферою [2] . Загроза безпеки визначається як сукупність умов і факторів, що створюють потенційну або реально існуючу небезпеку, пов'язану з витоком інформації та/або несанкціонованими та/або ненавмисними діями на неї.

Принцип «невидимості» заснований на тому, що існують недокументовані стани в системі, які ніяк не помітні для монітора безпеки і які дозволяють шкідливому коду маскуватися під штатний процес.

Під визначенням «руткіти» розуміється набір утиліт або спеціальний модуль ядра, які зловмисник використовує для прихованого вбудовування в операційні системи користувачів шкідливого програмного забезпечення(ВПО).

Під шкідливістю розуміється здатність програм завдати шкоди комп'ютерній системі за допомогою блокування, розкрадання, знищення і несанкціонованої передачі інформації.

Середа хмарних обчислень - це сукупність обчислювальних ресурсів у вигляді віртуальних машин, наданих користувачу 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. Розглянуті хмарні системи відносяться до типу «інфраструктура як сервіс», і для них характерно 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 впливів, що призводять до порушення функціонування компонентів інформаційного середовища.

Характерною особливістю сучасного середовища хмарних обчислень є активний характер суб'єктів та об'єктів інформаційної взаємодії. Це дозволяє розглядати цільову функцію системи безпеки як збереження конфіденційності, цілісності і доступності програмних та інфраструктурних сервісів, що надаються в режимі віддаленого доступу в умовах динамічного зміни стану обчислювальних ресурсів. В сучасних антивірусах, обманних системах захисту і сканерах безпеки не враховуються загрози, які реалізуються всередині периметра безпеки, Розробники програмно-технічних засобів захисту керуються власними уявленнями про створення прототипу продукту, використовуючи традиційні шаблони реалізації механізмів безпеки, саме тому найчастіше представлені на ринку засобів захисту інформації (ЗЗІ) володіють безліччю загальновідомих вразливостей навіть в умовах застосування новітніх технологій. Побудова перспективних механізмів забезпечення безпеки в середовищі хмарних обчислень пов'язується не з захистом від виявлених вразливостей, а полягає в можливості запобігання нових невідомих методів проведення атак, в розробці нових моделей загроз і методів запобігання або відображення комп'ютерних атак на інформаційні ресурси, які використовують можливості предикативній ідентифікації прихованих каналів і потенційно небезпечних процесів інформаційної взаємодії.

В умовах розвитку ринкової економіки фахівцями в різних країнах все більше уваги приділяється питанням розробки засобів захисту, що дозволяють протидіяти загрозам інформаційної безпеки 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 вразливим по ряду показників .

Причини, що зумовлюють виникнення вразливостей в середовищі хмарних обчислень, наступні:

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

На рис. 1 представлено статистичну вибірку опису динаміки змін атак вірусів.

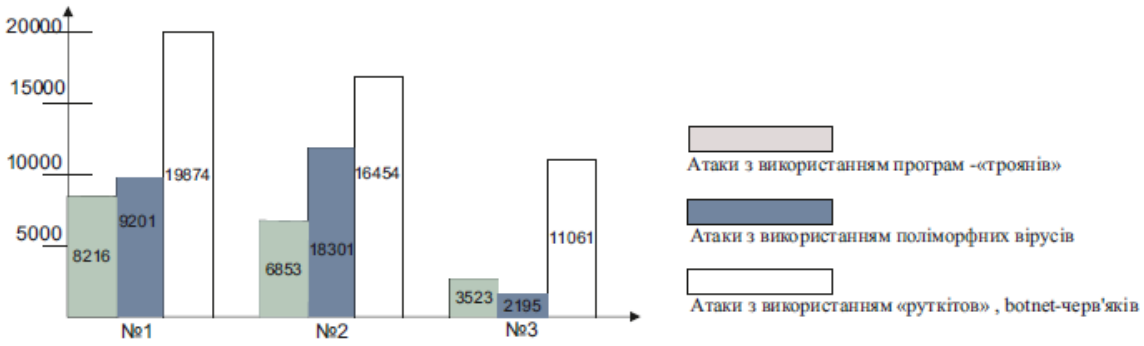

Рис. 1. Статистика атак з 2008 по 2016 рр.

Де: №1- з листопада 2008 р по січень 2010 р, № 2 - сукупні зміни з жовтня 2010 по липень 2012, № 3 - загальна кількість атак з вересня 2012 по січень 2016 .

Подальше розроблення нових технологій необхідно здійснювати на рівні протоколів взаємодії ОС і драйверів пристроїв, так як програмні модулі на зазначених інтерфейсних рівнях володіють привілейованими повноваженнями і можуть здійснювати довільні дії в операційних системах. Однією з найважливіших задач комп'ютерної безпеки є боротьба зі шкідливим програмним забезпеченням і зокрема підзавдання його виявлення. Всі методики виявлення можна розділити на 2 типи: методики виявлення відомого ВПО і методики виявлення невідомого ВПО .

Методи, засновані на експертних знаннях, використовуються для формалізації поняття «шкодочинність» і знань експертів в області дослідження шкідливих програм. Знання можуть бути пов'язані, наприклад, з тим, які дії є шкідливими (поведінковий аналіз), або які особливості структури можуть говорити про шкодочинності (статичний або динамічний структурний аналіз). Надалі ці формалізовані знання застосовуються для виявлення шкодочинності в досліджуваних даних.

Представниками даної групи методів є метод продукційних правил і метод поведінкових сигнатур.

В основу методу продукційних правил покладена модель подання знань у вигляді конструкцій «ЯКЩО-ТО». З допомогою таких правил можна вказати поодинокі ознаки шкідливості.

Метод сигнатур розроблено для поведінкового аналізу. За основу взято метод продукційних правил, який був адаптований для виявлення шкідливих послідовностей дій (тобто визначення переходу системи в «інфікований» стан).

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

Об'єднання різнорідних обчислювальних систем обумовлює реалізацію розширених механізмів захисту персональних даних користувачів, використання надійних алгоритмів шифрування, програмно-апаратних засобів контролю цілісності, створення довіреної

середовища завантаження. У середовищі хмарних обчислень багато користувачів, які запускають різні дистрибутиви ОС, тому необхідно розмежовувати канали обміну, фізичні та віртуальні ресурси у відповідність з рольовими політиками безпеки, щоб виключити пошкодження і розкрадання інформації, що захищається з різними рівнями доступу, несанкціонований доступ з боку зловмисника.

Планується також використання «хмарного сховища» від компанії Cleversafe. Масивні обсяги даних нарізають на частини і потім розподіляють по різним місцями розташування, або «вузлів зберігання». Хоча дані можуть знаходитися в чотирьох різних дата центрах по всій країні, вони можуть бути доступні в реальному часі з «окремих хмар». У даного виду зберігання даних кілька переваг. по-перше, це конфіденційність, окремі блоки данних не можуть бути розшифровані самі по собі, навіть якщо стороння особа отримало кілька таких частин. по-друге, на відміну від традиційних методів зберігання, немає ніякої необхідності, робити кілька копій вихідних даних, що дозволяє заощадити фінансові витрати.

Створення хмарної мережі отримало кодову назву «Хаддл». Передбачається розробка за участю компаній Mellanox, Тріні-мережі, Luxent Group нового 48-потового маршрутизатора InfiniBand Хмара VPI-перемикача (з вбудованою підтримкою апаратної віртуалізації), швидкість передачі в якому буде 100 Гб / с 56 Гб замість / с Infini-Band FDR. Також телекомунікаційне обладнання буде підтримувати повну апаратну віртуалізація 10-гігабітних Ethernet PCI-Express.

Створена трирівнева глобальна хмарна система(SpiderNetX), складається з наступних базових ланок:

1. Обчислювальні вузли суперпродуктивних комп'ютерних центрів на базі провідних науково-дослідних лабораторій (Массачусетський інститут, Університет Джорджії, Тихоокеанська дослідна лабораторія, Ліверморская національна дослідна лабораторія, Лабораторія спеціальних досліджень Trinix Агентства національної безпеки США, компанія IBM,компанії Cray Research Inc і SGI, обчислювальний центр S.C.O.M.P Пентагону, Комп'ютерний центр суперкластерний N-Куб Інститутустратегічних досліджень ЦРУ).

На обчислювальних вузлах високошвидкісних комунікаційних мереж суперкомп'ютерів стратегічного призначення (СКСН) встановлюються захищені «гібридні» ОС, відмінні від класичних операційних систем класу Unix або Windows NT, з розширеною апаратної ізоляцією виконання привілейованого коду, з підтримкою «безперервної» глобальної адресації фізичної пам'яті порядку 256 Терабайт і мультітредовой апаратно й архітектури: ОС Cray МТК для сегментів мережі Пентагону, Blacker ОС для сегментів мережі АНБ, ОС XTS для сегментів мережі ЦРУ.

2. Сервісні вузли з підтримкою мейнфреймів і стандартних кластерних систем під управлінням «класичних» Unix-подібних ОС (Red Hat Linux, SUSE Linux, Mandriva Linux, ALT Linux, IBM AIX, SGI IRIX,ШОС, Sun Solaris). Вони призначені для зберігання і обробки інформації на файлових серверах, забезпечення доступу до відкритих публікаціям науково-дослідних центрів, систем картотек Бібліотечних фондів а також для обробки пошукових запитів з клієнтських ЕОМ в соціальних мережах.

Сервісні вузли глобальної системи SpiderNetX включені в контур інформаційних систем освітніх установ США, Канади, Австралійської асоціації, Європейського Союзу (Великобританія, Франція, Німеччина, Італія, Швейцарія), країн Близького Сходу (Саудівська Аравія, ОАЕ), Центральної та Східної Азії (Індія, Китай, Японія, Південна Корея, Сінгапур), країн Прибалтики (Литва, Латвія, Естонія), Росії і країн СНД (Казахстан, Азербайджан, Україна). Основні інноваційні академічні за задумом дослідження уряду США проводитимуться на території США, Канади, Європи та Австралійської асоціації з метою зниження фінансових витрат на інноваційні проекти «нової ери суперкомп'ютерів» в якості технологічної платформи і сировинної бази виступають вигідні економічні зони Центральної та східної Азії. Дослідницький центр IBM в Нью-Делі (Індія), Шанхайська лабораторія Cray Inc (Китай), Об'єднаний центр комп'ютерних досліджень SGI Бейкер Сінгапуру, центр

стратегічних досліджень Минатома Японії, Міжвідомчий обчислювальний центр Університету Сеула (Південна Корея).

3. Клієнтські ЕОМ, робочі станції користувачів (операторів) глобальної розподіленої інформаційнною системою, підключені до локальних мереж освітніх установ і мають доступ в Інтернет, мобільні «тонкі» клієнти і персональні комп'ютери. На клієнтських обчислювальних засобах в країнах Близького Сходу, Центральної і Східної Азії, Європи, Росії та країнах СНД в основному встановлені ОС класу Windows NT.

Аналізатори мережевих вторгнень створюються, щоб забезпечити додатковий рівень захисту обчислювальної мережі, доповнюючи традиційні засоби захисту: міжмережеві екрани, кріптомаршрутизатори, сервери аутентифікації . Зловмисник під час здійснення атак намагається подолати систему захисту, використовуючи як методи «грубого злому», так і нові «руткіт» - технології для прихованого доступу до ресурсів операційних систем і спостереження за інформаційними потоками. Система аналізу захищеності покликані здійснювати збір даних про «аномальної» активності в системі і виявляти факти прихованого впливу на ресурси інформаційних систем, попереджати спроби здійснення несанкціонованого доступу (НСД).

Незважаючи на те, що ці системи не можуть виявляти атаку в процесі її розвитку, вони можуть визначити можливість реалізації атак . Виявлення атак здійснюється за допомогою аналізу реєстраційних журналів, баз даних аудиту або інформаційних потоків в режимі реального часу. Засоби виявлення атак дозволяють вдосконалити «класичні» підходи в області створення СЗІ за допомогою функціональної реалізації механізмів сигнатурного пошуку, підвищуючи рівень захисту обчислювальної мережі. Наприклад, засоби виявлення атак розпізнають спроби здійснення несанкціонованого доступу порушником , аналізую параметри переданих пакетів в мережі (прапори керування TCP / IP, час «життя» пакета, аномальні зміни розмірів переданих пакетів), здійснюють сигнатурний аналіз на наявність «характерних відбитків пальців» (відбитки пальців) у тактичних діях противника.

При цьому зазначені технічні засоби розширюють функціональність міжмережевих екранів, здійснюючи контроль доступу користувачів до ресурсів внутрішніх і зовнішніх сегментів локальних і глобальних телекомунікаційних систем.

У складі систем виявлення атак реалізовані криптографічні механізми контролю цілісності. Контроль цілісності дозволяє реалізувати стратегію ефективного моніторингу, сфокусовану на системах, в яких цілісність даних і цілісність процесів відіграє найважливішу роль .

Даний підхід дозволяє контролювати цілісність об'єктів файлової системи, реєструвати спроби здійснення НСД за допомогою зміни атрибутивних ознак ресурсів обчислювальних систем. Другим, не менш важливим, підходом є використання моделі адаптивного захисту інформації [3]. Модель адаптивних систем захисту розподілених систем дозволяє здійснювати гнучке налаштування компонентів СЗІ та оперативно реагувати на зовнішні дестабілізуючі дії з боку порушника в умовах, коли обстановка інформаційної протидії вкрай мінлива. При цьому можна привести аналогії з біологічного світу. Будь-яка форма життя має вроджені або набуті механізми адаптації до зовнішнього середовища проживання. У разі зміни стійких показників «еконіші» існування, організм прагне в найбільш короткі терміни оптимально підлаштується під нові умови середовища. Так і адаптивні системи захисту здійснюють зміну конфігурації СЗІ, налаштування її окремих компонентів з урахуванням сигнальних подій у відповідь на дії противника, підвищуючи рівень захищеності в критичні періоди здійснення активного вторгнення в комп'ютерні системи.

Компонент, який реалізує адаптивні властивості СЗІ, здійснює аналіз в режимі реального часу атак, отримуючи інформацію від аналізатора мережевих вторгнень, модулів МЕ, прогнозує появу нових класів вразливостей на основі емпіричних даних про вже відомі атаках і вносить поновлення в бази даних аудиту з урахуванням можливих (перспективних) атаки з боку зловмисника. Ключовим аспектом технології адаптивного захисту є перехід від принципу "виявлення і ліквідація НСД" до принципу .. "аналіз - прогнозування -

попередження - протидія" Дана технологія заснована на динамічному аналізі дій користувачів, контролі виконання програмного коду в комп'ютерних системах, контролю доступу до ресурсів ВС за допомогою детального аналізу інформації журналів аудиту та «міток» доступу монітора безпеки, виявленні неявних (прихованих) взаємодій користувачів і об'єктів доступу.

Дана технологія не дозволяє в повній мірі вирішувати проблему аналізу захищеності інформаційних систем з урахуванням застосування зловмисником програмних засобів прихованого впливу, алгоритмів і методів, що реалізують принцип «невидимості», оскільки враховує лише обмеження дій суб'єктів доступу і впливів шкідливого коду із застосуванням штатних засобів захисту.

Також до уваги береться можливість здійснення розподілених атак з використанням програмних агентів зловмисника. Програмний агент зловмисника може використовувати процесор до роботи легальних програм, тобто агент модифікує системні дані так, як потрібно йому, потім обробити запит і передати легальним програмами ту інформацію, яку йому потрібно.

Обманні системи захисту засновані на використання методів комп'ютерного обману. Наприклад, можна привести досить наочний приклад приховування структури (топології) обчислювальної мережі за допомогою програмно-технічних засобів захисту.

Застосування засобів, що реалізують камуфляж і дезінформацію, перешкоджає успішному здійсненню НСД зловмисником, оскільки порушник у разі використання облудної системи захисту, змушений витрачати на альтернативні шляхи здійснення вторгнення, оскільки у нього немає достовірної інформації про те, чи працює він з реальною операційною системою або є учасником «гри», запропонованої йому в якості «приманки» (тактика залучення уваги). Даний метод реалізований в продукті Cybercop Sting .

Найбільш поширеним пакетом, які реалізують технології обманних систем зарубіжними компаніями в рамках проведення досліджень в області застосування перспективних технологій захисту, є програмний продукт ДТК (Обман Toolkit).

Концепція створення даного продукту належить провідним експертам в галузі комп'ютерної безпеки Масачусітського технологічного інституту - Кліффу Столл і Біллу Чезвіку. Даний засіб розроблено з тією метою, щоб ввести в оману автоматизовані засоби аналізу захищеності шляхом створення помилкових вразливостей, що дозволить своєчасно виявити спроби несанкціонованого доступу і протиставити їм ефективні засоби захисту і, можливо, виявляти атакуючого .

Висновки. 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.

ЛІТЕРАТУРА:

1. Критически важные объекты и кибертерроризм. Часть 1. Системный подход к организации противодействия / / О.О. Андреев [и др.]. Под ред. В.А. Васенина. – М.:

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

4. Larochelle , D. Statically detecting likely buffer overflow vulnerabilities / D,Larochelle and D. Evans // In USENIX Security Symposium,. - 2001. - pp. 177-190.

5. Bush , W.R.. A static analyzer for finding dynamic programming errors W. R. Bush, I D. Pincus, and D. J. Sielaff / In Proceedings of Software Practice and Experience . - 2000.- pp. 775-802.

6. Benjamin , V. Context Sensitivity for Bug Detection in C Programs / V. Benjamin Livshits and Monica S. Lam // In Proceedings of the 11th ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE-11). - 2003. – pp. 123-125.

7. Milanova , A. Precise and Practical Flow Analysis of Object-Oriented Software/A. A. Milanova // Ph.D thesis, Rutgers University, Available as Techical Report DCS-TR-539. - 2003. – pp. 234-242.

REFERENCES:

1. Kriticheski vazhnyie ob'ektyi i kiberterrorizm. Chast 1. Sistemnyiy podhod k organizatsii protivodeystviya / / O.O. Andreev [i dr.]. Pod red. V.A. Vasenina. – M.:

2. 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.

3. Olifer , V.G.. Kompyuternyie seti / V.G. Olifer. - SPb.: Izd- vo Piter, 2004. – c. 198-199 .

4. Larochelle , D. Statically detecting likely buffer overflow vulnerabilities / D,Larochelle and D. Evans // In USENIX Security Symposium,. - 2001. - pp. 177-190.

5. Bush , W.R.. A static analyzer for finding dynamic programming errors W. R. Bush, I D. Pincus, and D. J. Sielaff / In Proceedings of Software Practice and Experience . - 2000.- pp. 775-802.

6. Benjamin , V. Context Sensitivity for Bug Detection in C Programs / V. Benjamin Livshits and Monica S. Lam // In Proceedings of the 11th ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE-11). - 2003. – pp. 123-125.

7. Milanova , A. Precise and Practical Flow Analysis of Object-Oriented Software/A. A. Milanova // Ph.D thesis, Rutgers University, Available as Techical Report DCS-TR-539. - 2003. – pp. 234-242.

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

Козак И.В., к.воен.н., доц. Пашков С.А., к.т.н., доц. Огнєвой А.В.

АНАЛИЗ ПРОБЛЕМ ЗАЩИТЫ ИНФОРМАЦИИ В СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

В статье проведен анализ существующих угроз, реализуемых с использованием скрытых каналов и декларируемых возможностей программного обеспечения (ПО). 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.

Особое внимание уделено анализу недостатков современных технологий защиты информации в среде облачных вычислений, которые не учитывают динамический характер предоставленных прикладных и системных программных сервисов.

Ключевые слова: облачные вычисления, кибербезопасность, информационная безопасность, скрытые угрозы, компьютерные системы.

Kozak I.V., Ph.D Pachkov S.A., Ph.D Ognjevyj A.V.

ANALYSIS OF THE PROBLEMS OF INFORMATION PROTECTION IN CLOUD COMPUTING ENVIRONMENT

The article analyzes the existing threats are realized using covert channels and the declared capabilities of software (PO). We show how the implementation of hidden threats allows malicious code disguised as a systematic process, harming the security of cloud computing environments using blocking, theft, destruction or unauthorized transfer of information.

Particular attention is paid to analysis of the shortcomings of modern technologies of information security in cloud computing environments that do not take into account the dynamic nature of the provided software applications and system services

Keywords: cloud computing, cyber security, information security, hidden threats, a computer system.