УДК 004.056.52
UDC 004.056.52
DOI: 10.33744/2308-6645-2020-1-46-427-436

ІНФОРМАЦІЙНА БЕЗПЕКА ТЕХНОЛОГІЇ ХМАРНИХ ОБЧИСЛЕНЬ

Червякова Т.І., кандидат технічних наук, Національний транспортний університет, м. Київ, Україна, cherti2015@gmail.com, orcid.org/0000-0002-3672-9173

INFORMATION SECURITY OF CLOUD COMPUTING TECHNOLOGY

Cherviakova T.I., Ph.D., National Transport University, Kyiv, Ukraine, cherti2015@gmail.com, orcid.org/0000-0002-3672-9173

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕХНОЛОГИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Червякова Т.И., кандидат технических наук, Национальный транспортный университет, г. Киев, Украина, cherti2015@gmail.com, orcid.org/0000-0002-3672-9173

Постановка проблеми.

Останнім часом все більшого поширення набуває технологія хмарних обчислень, що передбачає віддалений (в тому числі через Інтернет) доступ користувачів до сховищ даних, обчислювальних ресурсів і програмних додатків [1, 2].

Клієнти хмарних сервісів можуть істотно зменшити вартість зберігання даних і використання обчислювальних потужностей, використовуючи загальнодоступні мережеві сховища і обчислювальні ресурси. Постачальник послуг об'єднує ресурси для обслуговування широкого кола споживачів в єдиний пул для динамічного і ефективного перерозподілу потужностей між споживачами в умовах постійної зміни попиту на потужності.

Різноманітність пристроїв, що використовуються в хмарних обчисленнях, радикальним чином знижують вартість використання обчислювальних ресурсів [3]. Зменшена вартість розподілених обчислень, спільної пам'яті та систем зберігання даних фундаментально змінюють економіку обробки даних, роблячи хмарні обчислення вельми привабливими для багатьох клієнтів.

При цьому часто не береться до уваги той факт, що при передачі даних у хмару власник практично позбавляється можливості контролювати їх безпеку [4], а провайдери не поспішають брати на себе відповідальність за їх безпеку [5].

Аналіз останніх досліджень і публікацій.

Проблемам інформаційної безпеки хмарних обчислень присвячені дослідження таких вітчизняних науковців: Г.С. Гриджука, Є.С Бондаря., І.В. Бондаренка, І.Д. Горбенка, О.О.Гудзовати, Ю.Л. Поночовного, а також зарубіжних учених таких, як Бердник А.В., Ісаєв Е.А., Корнілов В.В., Brenton C., Jansen W, Grance T., Reshetova E., Karhunen J., Nyman T., Asokan N. та ін. Однак, подальших досліджень потребує розробка стратегії інформаційної безпеки технології хмарних обчислень.

Цілі статті – аналіз теоретичних і практичних аспектів інформаційної безпеки технології хмарних обчислень, визначення їх принципів і перспектив.

Виклад основного матеріалу дослідження.

Одним із основних підходів до реалізації хмарної інфраструктури є технологія віртуалізації – надання обчислювальних ресурсів, абстрагованих від їх реальної апаратної реалізації, наприклад, одночасне використання декількох, ізольованих одна від одної, операційних систем (ОС) і додатків на одному комп'ютері. Сукупність комп'ютерних ресурсів, що емулює роботу окремих компонентів апаратного або програмного забезпечення (ПЗ), або комп'ютера, прийнято називати віртуальною машиною (ВМ). Наявність декількох ВМ на одному реальному комп'ютері забезпечує можливість незалежної роботи на одному фізичному сервері (вузлі) декількох операційних систем і додатків.

На даний час існує дві основні технології створення систем хмарних обчислень шляхом віртуалізації серверів. У першому підході віртуалізація здійснюється за допомогою гіпервізора – програмної надбудови над основною ОС, яка відокремлює віртуальні машини від сервера і в міру необхідності динамічно виділяє обчислювальні ресурси для кожної ВМ (Amazon, Azure, VMWare) [6].

Другий підхід має переваги з точки зору обчислювальної продуктивності системи і економії дискових ресурсів завдяки використанню контейнерами ядра основної системи. При цьому користувачі обмежені в виборі ОС виключно дистрибутивами сімейства GNU/Linux, що в більшості випадків сприймається як суттєвий недолік контейнерної віртуалізації. Водночас, суттєвий виграш у продуктивності дозволяє в даному випадку використовувати ресурси хмари навіть для високоефективних обчислень [7]. Останні роки Amazon і Azure, крім традиційної віртуалізації на основі гіпервізора, почали надавати послуги на основі контейнерних технологій [8]. Google використовували дану технологію спочатку як основну [9].

Другим недоліком до недавнього часу були серйозні проблеми в безпеці: оскільки кожен контейнер має доступ до ядра основної системи, то потенційний зловмисник міг отримати привілейовані права в основній системі, зламавши один з контейнерів у хмарі. Слід зазначити, що в останніх розробках системи віртуалізації LXC з'явилася можливість запускати непривілейовані контейнери, зламавши які зловмисник отримає тільки обмежені права користувача в основній системі [10].

У зв'язку з технологічними особливостями, що використовуються для побудови структури хмарних обчислень, до стандартних типів загроз, які є наслідком розміщення ресурсів на фізичних серверах, додалися складності, пов'язані з контролем хмарного середовища віртуалізації, трафіку між гостьовими машинами та розмежуванням прав доступу. Більш того, розподілена і відкрита структура хмарних обчислень з мультидоменною структурою, розрахованої на багатьох користувачів, стала дуже привабливою мішенню для потенційних зловмисників.

Архітектура хмарних сервісів складається з трьох взаємозалежних рівнів: інфраструктура, платформа і додатки. Кожен з цих рівнів може бути уразливим до програмних і конфігураційних помилок, яких припустилися користувачі або провайдери сервісу. Система хмарних обчислень може піддаватися декільком видам загроз безпеки, включаючи загрози цілісності, конфіденційності та доступності її ресурсів, даних і віртуальної інфраструктури, які можуть бути використані нецільовим чином, наприклад, в якості майданчика для поширення нових атак [11].

Зберігання даних у хмарі означає, що дані містяться на загальнодоступних серверах. Якщо компанія перейде в хмару без урахування непередбачених наслідків, критичні корпоративні дані, такі, як, наприклад, інформація про клієнтів або інтелектуальна власність, піддадуться підвищеному ризику. При цьому юридичну відповідальність за збереження інформації, як і раніше, несе організація, що розмістила ці дані в хмарі, а не провайдер хмарних послуг.

Інша серйозна проблема захисту даних у хмарі – це нездатність для клієнта хмарних послуг самому проводити аудит і контролювати події служби безпеки, наприклад, за допомогою перевірки лог-файлів. Це може серйозно обмежити можливості з пошуку загроз, які призвели до порушення безпеки системи.

У хмарних обчисленнях важливу роль відіграє технологія віртуалізації. Однак принципи віртуалізації містять потенційні загрози інформаційній безпеці хмарних обчислень, наприклад, пов'язані з використанням загальних сховищ даних різними ВМ. Кожна ВМ зберігається у вигляді образу, який являє собою окремий файл. Розміри цих файлів можуть бути змінені в залежності від поточних потреб користувача сервісу. Зменшення розміру розділу однією з ВМ хмари і збільшення розділу іншої можуть привести до того, що фізичні сектори, що містять інформацію про віддалені файли, перемістяться з однієї ВМ на іншу. В результаті користувач другої ВМ може отримати доступ і відновити дані, які раніше належали іншій організації. Одним із можливих рішень є шифрування всієї інформації. В цьому випадку зашифрована інформація не зможе бути відновлена без відповідних ключів [12]. Однак слід враховувати, що шифрування може призвести до використання додаткових обчислювальних ресурсів і значно уповільнювати процес читання і запису даних.

На противагу фізичному серверу, ВМ з такою ж ОС і додатками з ідентичними налаштуваннями схильна до більшого ризику. Якщо провайдер хмари резервує, управляє або маніпулює ВМ для клієнтів на основі своїх власних конфігураційних шаблонів, то контроль доступу і базові конфігурації не відповідатимуть таким у власному дата-центрі організації. Навіть в рамках одного провайдера хмари, може виникати ситуація, коли налаштування примірника ВМ в одному розміщенні будуть відрізнятися від налаштувань в іншому розміщенні [13].

ВМ динамічні. Вони клонуються і можуть переміщатися між фізичними серверами. Дана мінливість впливає на розробку цілісності системи безпеки. Однак уразливості ОС або додатків у віртуальному середовищі поширюються безконтрольно і часто проявляються через деякий проміжку часу (наприклад, при відновленні з резервної копії). У середовищі хмарних обчислень важливо надійно зафіксувати стан захисту системи, незалежно від її місця розташування.

Сервери хмарних обчислень і локальні сервери використовують одні й ті самі ОС і додатки. Для хмарних систем висока загроза віддаленого злому або зараження шкідливим ПЗ. Система виявлення та запобігання вторгненням повинна бути здатною виявляти шкідливу активність на рівні ВМ, незалежно від їх розташування в хмарному середовищі.

Навіть коли ВМ вимкнена, вона також наражається на небезпеку зараження. Для цього цілком достатньо доступу до сховища образів ВМ через мережу. При цьому на вимкненій ВМ неможливо запустити захисне програмне забезпечення. В даному випадку має бути реалізованим захист не тільки всередині кожної ВМ, а й на рівні гіпервізора.

При використанні хмарних обчислень периметр мережі розмивається або зникає. Це призводить до того, що менш захищена частина мережі визначає загальний рівень захищеності. Для розмежування сегментів з різними рівнями довіри в хмарі ВМ повинні самі забезпечувати себе захистом, переміщаючи мережевий периметр до самої ВМ. Корпоративний firewall (міжмережевий екран) – основний компонент для впровадження політики IT-безпеки і розмежування сегментів мережі – не в змозі вплинути на сервери, розміщені в хмарних середовищах [14].

Стандартно виділяють три основні завдання інформаційної безпеки: конфіденційність, цілісність і доступність [15]. Конфіденційність – це приховування інформації і ресурсів. Цілісність – це достовірність даних або ресурсів, зазвичай пов'язана із запобіганням будь-яких некоректних або неавторизованих змін. Доступність визначається здатністю використовувати інформацію або ресурси [16]. Принципово вважається, що доступ до даних можуть отримати тільки особи, що пройшли аутентифікацію в якості клієнта сервісу і власника саме цих даних.

Один з основних моментів, який необхідно враховувати стосовно безпеки в хмарі, полягає в тому, що відповідальність за використання ресурсів поділяється між клієнтом і постачальником хмарного сервісу. І необхідно розуміти, де закінчується відповідальність провайдера хмарних обчислень і починається відповідальність клієнта.

При побудові складних систем (різновидом яких є хмари) застосовують архітектурну концепцію багаторівневої безпеки (Defense-in-Depth) – механізм, який використовує кілька рівнів захисту, щоб збільшити витрати часу атакуючого на злам системи, а також підрахувати кількість спроб зламу для прийняття рішення про блокування атакуючого [17].

Відповідно при побудові системи безпеки середовища хмар також можна виділити свої шари контролю та доступу. Хмара комбінує можливості користувача і постачальника, брандмауери і різновиди способів ізоляції. При цьому окремі елементи безпеки можуть контролюватися користувачем незалежно від провайдера (рис. 1).

Рисунок 1 – Багаторівнева система безпеки хмар на прикладі трьох моделей хмарних сервісів [18]

Figure 1 – Multi-level cloud safety system on the example of three models of cloud services [18]

NIST в своїй спеціальній публікації [4] виділяє три моделі хмарних обчислень:

інфраструктура як сервіс (IaaS);

платформа як сервіс (PaaS);

програмне забезпечення як сервіс (SaaS).

При цьому для кожної моделі хмарних обчислень управління даними змінюється. Так, в різних сервісах клієнтом контролюються різні шари безпеки незалежно від провайдера [18].

У моделі IaaS (наприклад, IBM SoftLayer або Amazon Web Services) на стороні замовника можна побудувати свої власні технічні засоби забезпечення безпеки. Клієнт може мати повний контроль над реальною конфігурацією сервера, що гарантує йому більший контроль ризиків безпеки оточення і даних.

У моделі PaaS (IBM Bluemix, Microsoft Windows Azure) постачальник управляє лише апаратною платформою і операційною системою, що обмежує можливості підприємства замовника в управлінні ризиками на цих рівнях.

У моделі SaaS (Salesforce.com, Google) платформа і інфраструктура повністю управляється провайдером хмарних послуг. У можливостях управління клієнт виявляється обмеженим тільки мінімальним набором налаштувань конфігурації програми під свої потреби.

Відповідальність постачальника хмарного сервісу починається з фізичної безпеки і безпеки середовища. Цей рівень безпеки – високорівневий, оскільки пов'язаний з керованістю хмарою як єдиною інформаційною системою. Саме постачальник хмарного сервісу здійснює експлуатацію фізичних серверів центрів обробки даних. Тому клієнт повинен розглянути наступні ключові моменти: фізичний доступ персоналу до серверів і мережевої інфраструктури; засоби пожежної сигналізації та пожежогасіння; кліматичний і температурний контроль над серверами й іншими апаратними засобами; знищення пристроїв зберігання даних, виведених з експлуатації.

На відміну від фізичної безпеки, мережева безпека, в першу чергу, являє собою побудову надійної моделі загроз, що включає в себе захист від вторгнень і міжмережевий екран. Використання брандмауера має на увазі роботу фільтра по розмежуванню внутрішніх мереж ЦОД на підмережі з різним рівнем довіри. Це можуть бути окремо сервери, доступні з Інтернету, або сервери з внутрішніх мереж.

Доступ через Інтернет до управління обчислювальною потужністю хмари – одна з ключових характеристик хмарних обчислень. Тому, розмежування контролю доступу та забезпечення прозорості змін на системному рівні є одними з головних критеріїв захисту.

Аналогічним чином на загальний рівень безпеки впливає вибір моделі розгортання хмарного середовища: приватна хмара (інфраструктура, підготовлена для ексклюзивного використання єдиною організацією); публічна хмара (інфраструктура, призначена для вільного використання широким колом користувачів); суспільна хмара (вид інфраструктури, призначений для використання конкретною спільнотою споживачів з організацій, що мають спільні завдання); гібридна хмара (комбінація двох або більше різних хмарних інфраструктур).

До ключових особливостей приватних хмар в структурі забезпечення інформаційної безпеки можна віднести:

- відповідальність клієнта за інфраструктуру;
- можливість детального налаштування управління безпеки;
- добра видимість внутрішньоденних операцій;
- легкий доступ до системних логів і політикам;
- додатки і дані залишаються всередині мережевого екрану.

Прийнято вважати, що приватні хмари є найбільш безпечними, оскільки дозволяють впровадити власні засоби шифрування і захисту ще на етапі їх створення, а також залишити дані в існуючій інфраструктурі компанії. Однак, якщо дані не захищені належним чином в хмарі, вони можуть бути втрачені або пошкоджені незалежно від того, чи хмара приватна або публічна. Зокрема, недобросовісні особи всередині компанії, що мають довірений доступ до системи, можуть переглядати, пошкоджувати і викрадати незахищені дані.

Внутрішні загрози не є новими типами загроз, але при переході корпоративних дата-центрів в віртуальні традиційні механізми контролю доступу стають менш ефективними через непристосованість до віртуального простору. Наприклад, коли потрібно встановити екземпляр бази даних на новий фізичний сервер, застосовуються процедури управління змінами. Управління змінами являє собою процес прогнозування і планування майбутніх змін, реєстрації всіх потенційних змін для детального вивчення, оцінки наслідків, схвалення або відхилення, а також організації моніторингу і координації виконавців, що реалізують зміни в проекті. У віртуальній приватній хмарі новий

екземпляр бази даних може бути створений простим клонуванням вже існуючого віртуального сервера. Якщо дані з захищеного сервера передаються на незахищений, то ці дані зможуть переглянути користувачі, що мають менші права доступу в цій приватній хмарі.

Особливу увагу слід приділяти контролю трафіку між віртуальними серверами в хмарі. Традиційні засоби моніторингу працюють з використанням віддзеркалення трафіку з портів мережевих пристроїв і сенсорів, які здатні захоплювати і аналізувати цей трафік. Однак канали передачі даних між ВМ створюються в гіпервізорі. Шкідливий трафік і дані можуть переміщатися між ВМ без виходу в реальну мережу, що означає, що атака буде не помічена традиційними інструментами.

Дані, що зберігаються на вимкнених ВМ, також є уразливими у випадках, коли в основній ОС, на якій вони розміщуються, контроль доступу не налаштований належним чином, або не встановлені оновлення, що виправляють критичні уразливості.

На іншому полюсі (в бік зменшення безпеки) прийнято розташовувати публічні хмари. Можна виділити такі особливості публічних хмар:

- за інфраструктуру відповідає провайдер;
- менша налаштованість управління безпекою;
- немає видимості внутрішньоденних операцій;
- важкий доступ до логів і політикам;
- додатки і дані використовуються публічно.

Використовуючи публічну хмару, організації можуть скористатися інфраструктурою провайдера в хмарі (IaaS), платформою (PaaS) і програмним забезпеченням (SaaS). Дані зберігаються в середовищі хмарного провайдера з використанням орендованої інфраструктури комерційних ЦОД. У більшості випадків економія коштів в публічній хмарі досягається за рахунок більш ефективного використання загальних фізичних ресурсів. Це може означати як надання клієнтам різних ВМ, розміщених на одному й тому ж фізичному сервері, так і організаціям доступу до одного й того ж сервісу або додатку під різними обліковими записами. Наприклад, популярний хмарний CRM-додаток salesforce.com є прикладом надання одного й того ж сервісу різним клієнтам з використанням унікальних логінів для запобігання несанкціонованого доступу. При цьому дані різних користувачів виявляються перемішаними на одному сховищі. У будь-якому випадку при використанні віртуалізації доводиться брати до уваги весь комплекс проблем інформаційної безпеки, пов'язаний з цією технологією.

Звичайно, в рамках публічної хмари можливим є надання клієнту цілком окремого, виділеного комп'ютерного ресурсу, що, зокрема, дає можливість більш якісного моніторингу та аудиту. Однак такий додатковий рівень комфорту в забезпеченні безпеки часто супроводжується істотним збільшенням ціни використання хмарних ресурсів, що може в цілому знизити переваги таких перед власним дата-центром [13].

Класичні загрози інформаційній безпеці в публічній хмарі стають особливо актуальними. Існують і зовнішні загрози безпеки, такі як, наприклад, віддалені хакерські атаки. І, навіть, коли сховище даних досить добре захищене від зовнішніх атак, а контроль і розмежування доступу надає тільки мінімальні повноваження особливо довіреним особам, все ще залишаються відкритими питання безпеки при передачі даних між клієнтом і хмарною інфраструктурою. Сьогодні існує безліч стандартів і технологій передачі даних по інформаційних мережах і завдання забезпечення безпеки інформації в них є абсолютно нетривіальною, особливо в разі використання бездротових мереж. Зловмисники можуть перехопити дані безліччю способів, наприклад за допомогою підроблених серверів доменних імен, перехоплення маршрутів і трафіку при використанні співробітниками компанії не довірених хмар [19] і громадських Wi-Fi точок доступу та ін.

Організації можуть підвищити рівень безпеки при використанні гібридного підходу до хмарних обчислень, який поєднує в собі публічні та приватні хмари. Частина даних, які класифікуються організацією як найбільш критичні, залишаються в приватній хмарі, тоді як всі інші дані зберігаються в публічній хмарі.

Хоча цей підхід може гарантувати більшу безпеку, ніж стандартна модель публічної хмари, гібридні хмари несуть в собі ті ж ризики, що й приватні та публічні хмари у випадках неправильного їх використання. Збереження критично важливих даних усередині підприємства вимагає залучення механізмів і процедур, які гарантують, що ці дані не потраплять в публічну хмару.

Таким чином, для хмарних технологій спостерігається зворотна залежність: зі збільшенням ступеня відкритості технології, гнучкості роботи з нею і універсальності доступу зменшується захищеність системи і ускладняється методика забезпечення її безпеки.

Для того, щоб створити більш безпечне середовище хмарних обчислень, організації можуть почати з простих кроків, наприклад, з розробки політики та процедури безпеки, підвищення прозорості у використанні хмарних додатків, платформ та інфраструктури і захисту даних з шифруванням і посиленням процедури доступу до елементів управління, таких як багатофакторна аутентифікація [20].

IT-організації повинні зосередитись на посиленні контролю доступу користувачів методом багатофакторної аутентифікації. Це ще більш важливо для компаній, які дають третім сторонам і постачальникам доступ до своїх даних у хмарі. Багатофакторні рішення аутентифікації, керовані централізовано, забезпечать більш безпечний доступ до всіх програм і даних, незалежно від того, чи знаходяться вони в хмарі або в локальній мережі [21].

Найбільш ефективним і універсальним способом забезпечення захисту даних, їх конфіденційності і цілісності – це використання шифрування даних при їх передачі по інформаційних мережах і при зберіганні всередині хмари. Наприклад, в керівництві по інформаційній безпеці [22], розробленому Альянсом безпеки хмар, стверджується, що шифрування надає переваги найменшої залежності як від провайдера хмарного сервісу, так і від експлуатаційних помилок.

Захист даних, заснований на шифруванні, робить ці дані марними для будь-якої особи, що не має ключів для їх дешифрування. І не важливо, знаходяться ці дані в процесі передачі або зберігання, вони залишаються захищеними. Власник ключів шифрування підтримує безпеку даних і приймає рішення, кому і до яких даних надавати доступ. Процедура шифрування може бути вбудована в існуючий робочий процес хмарних сервісів. Наприклад, адміністратор може зашифровувати всі дані резервного копіювання перед відправкою їх в хмарне сховище. Співробітник організації може захистити корпоративну інтелектуальну власність, перш ніж покласти її в приватну хмару. Представник компанії може зашифрувати особисті контракти клієнтів, перш ніж відправити їх в спільне робоче місце в публічній хмарі.

Висновки.

Одним з універсальних способів забезпечення захисту даних в хмарі є вибір рішення безпеки, заснованого на шифруванні даних на рівні файлів перш ніж вони покинуть довірену зону. IT-адміністратори і користувачі можуть частково повернути собі контроль над забезпеченням безпеки своїх даних, використовуючи рішення захисту, засновані на шифруванні даних. Використання відповідних методів шифрування запобігає неавторизованому доступу до даних незалежно від того, де вони знаходяться (в процесі передачі або зберігання в хмарі), і дозволяють організаціям використовувати переваги хмарних обчислень, не піддаючи важливі дані ризику або зводячи цей ризик до мінімуму.

ПЕРЕЛІК ПОСИЛАНЬ

1. Лахно В.Д. Развитие информационно-коммуникационных технологий в Пущинском научном центре РАН. / В.Д. Лахно, Е.А. Исаев, В.Д. Пугачев, А.Ю. Зайцев, Н.С. Фиалко, С.Д. Рыкунов, М.Н. Устинин. // Математическая биология и биоинформатика. – 2012. – Т. 7, № 2. – С. 529–544.
2. Antonopoulos N., Gillam L. Cloud Computing: Principles, Systems and Applications. London: Springer-Verlag, 2010. – 379 p.
3. Исаев Е.А., Корнилов В.В. Проблема обработки и хранения больших объемов научных данных и подходы к ее решению. // Математическая биология и биоинформатика. – 2013. – Т. 8, № 1. – С. 49–65.
4. Jansen W, Grance T. Guidelines on Security and Privacy in Public Cloud Computing. 2011. – 80 p. (NIST Special Publication 800-144). URL: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf
5. Amazon Web Services Customer Agreement. Website of Amazon Web Services. 2008. URL: http://aws-portal.amazon.com/gp/aws/developer/terms-and-conditions.html
6. White J.S., Pilbeam A.W. A survey of virtualization technologies with performance testing. arXiv.org: Cornell University Library. URL: http://arxiv.org/pdf/1010.3233.pdf
7. Xavier M.G., Neves M.V., Rossi F.D., Ferreto T.C., Lange T., De Rose C.A.F. Performance Evaluation of Container-Based Virtualization for High Performance Computing Environments. In: 21st Euro. Int. Conf. on Parallel, Distrib. & Network- based Processing. IEEE, 2013. – P. 233–240.
8. Morabito R. Power Consumption of Virtualization Technologies: an Empirical Investigation. arXiv.org: Cornell University Library. URL: http://arxiv.org/pdf/1511.01232v1.pdf

9. Cacciatore K., Czarkowski P., Dake S., Garbutt J., Hemphill B., Jainschigg J., Moruga A., Otto A., Peters C., Whitaker B.E. Exploring Opportunities: Containers and OpenStack. OpenStack White Paper. 2015. – 19 p. URL: https://www.openstack.org/assets/pdf-downloads/Containers-and-OpenStack.pdf

10. Reshetova E., Karhunen J., Nyman T., Asokan N. Security of OS-level virtualization technologies. arXiv.org: Cornell University Library. URL: http://arxiv.org/pdf/1407.4245v1.pdf

11. Patel A., Taghavi M., Bakhtiyari K., Junior J.C. An intrusion detection and prevention system in cloud computing: A systematic review. Journal of Network and Computer Applications. 2013. V. 36. – P. 25–41.

12. Brenton C. The basics of virtualization security. Cloud Security Alliance, 2011. – 17 p. URL: https://cloudsecurityalliance.org/wp-content/uploads/2011/ 11/virtualization-security.pdf

13. Kelley D. How Data-Centric Protection Increases Security in Cloud Computing and Virtualization Security Curve. Website of Cloud Security Alliance. 2011. – P. 1–6. URL: https://cloudsecurityalliance.org/wp- content/uploads/2011/ 11/DataCentricProtection_intheCloud.pdf

14. Бердник А.В. Проблемы безопасности облачных вычислений. Анализ методов защиты облаков от cloud security alliance / А.В. Бердник. // Альманах современной науки и образования. – Тамбов: Грамота, 2013. – № 10. – С. 35–38.

15. Lubacz J., Mazurczyk W., Szczypiorski K. Principles and Overview of Network Steganography. Communications Magazine. IEEE, 2014. V. 52. № 5. P. 225–229. URL: http://arxiv.org/pdf/1207.0917.pdf

16. Bishop M. Introduction to Computer Security, 1st ed. Boston: Pearson Education, 2004. –747 p.

17. Prescott E. Small. Defense in Depth: An Impractical Strategy for a Cyber World. SANS Institute, 2011. – P. 2– 4. URL: https://www.sans.org/reading- room/whitepapers/assurance/defense-depth-impractical-strategy-cyber-world-33896

18. Ржаиби В. Избавьтесь от опасений относительно безопасности данных в облаке. IBM developer Works, 2015. – 16 p. URL: https://www.ibm.com/developerworks/ru/library/dm-1408datasecuritycloud/dm-1408datasecuritycloud-pdf.pdf

19. Avoiding the hidden Costs of the Cloud: report of Symantec Corporation. 2013. – P. 1–11. URL: www.symantec.com/content/en/us/about/media/pdfs/b-state-of-cloud-global- results-2013.en-us.pdf

20. The Challenges of Cloud Information Governance: A Global Data Security Study: Ponemon Institute Research Report. 2014. P. 1–30. URL: http://www2.safenet- inc.com/cloud-security-research/SafeNet-Cloud-Governance.pdf

21. Sultan N. Making use of cloud computing for healthcare provision: Opportunities and challenges. International Journal of Information Management. 2014. – V. 34. – P. 177–184.

22. Hoff Ch. In: Security guidance for critical areas of focus in cloud computing. 2011. – P. 12–20. URL: https://cloudsecurityalliance.org/ guidance/csaguide.v3.0.pdf

REFERENCES

1. Lakhno, V.D. (2012). Razvitie informatsionno-kommunikatsionnykh tekhnolohii v Pushchinskom nauchnom tsentre RAN.[Development of information and communication technologies in the Pushchinsky Scientific Center of the Russian Academy of Sciences]. / V.D. Lahno, E.A. Isaev, V.D. Pugachev, A.Yu. Zaytsev, N.S. Fialko, S.D. Ryikunov, M.N. Ustinin. // Matematicheskaia biologiia i bioinformatika.– T. 7, # 2. – S. 529–544. [in Russian]

2. Antonopoulos, N., Gillam, L. (2010). Cloud Computing: Principles, Systems and Applications. London: Springer-Verlag. – 379 p.

3. Isaev, E.A., Kornilov, V.V. (2013). Problema obrabotki i khraneniia bolshikh obiemov nauchnykh danykh i podkhody k ee resheniiu. [The problem of processing and storing large amounts of scientific data and approaches to its solution]. Matematicheskaia biolohiia i bioinformatika. T. 8. № 1. – S. 49–65. [in Russian]

4. Jansen, W., Grance, T. (2011). Guidelines on Security and Privacy in Public Cloud Computing.– 80 p. (NIST Special Publication 800-144). URL: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

5. Amazon Web Services Customer Agreement. Website of Amazon Web Services. 2008. URL: http://aws-portal.amazon.com/gp/aws/developer/terms-and-conditions.html

6. White J.S., Pilbeam A.W. A survey of virtualization technologies with performance testing. arXiv.org: Cornell University Library. URL: http://arxiv.org/pdf/1010.3233.pdf

7. Xavier, M.G., Neves, M.V., Rossi, F.D., Ferreto, T.C., Lange, T., De Rose, C.A.F. (2013). Performance Evaluation of Container-Based Virtualization for High Performance Computing Environments. In: 21st Euro. Int. Conf. on Parallel, Distrib. & Network- based Processing. IEEE. – P. 233–240.

8. Morabito R. Power Consumption of Virtualization Technologies: an Empirical Investigation. arXiv.org: Cornell University Library. URL: http://arxiv.org/pdf/1511.01232v1.pdf

9. Cacciatore, K., Czarkowski, P., Dake, S., Garbutt, J., Hemphill, B., Jainschigg, J., Moruga, A., Otto, A., Peters, C., Whitaker, B.E. (2015). Exploring Opportunities: Containers and OpenStack. OpenStack White Paper. – 19 p. URL: https://www.openstack.org/assets/pdf-downloads/Containers-and-OpenStack.pdf

10. Reshetova E., Karhunen J., Nyman T., Asokan N. Security of OS-level virtualization technologies. arXiv.org: Cornell University Library. URL: http://arxiv.org/pdf/1407.4245v1.pdf

11. Patel, A., Taghavi, M., Bakhtiyari, K., Junior, J.C. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. Journal of Network and Computer Applications. V. 36. – P. 25–41.

12. Brenton, C. (2011).The basics of virtualization security. Cloud Security Alliance. – 17 p. URL: https://cloudsecurityalliance.org/wp-content/uploads/2011/ 11/virtualization-security.pdf

13. Kelley, D. (2011). How Data-Centric Protection Increases Security in Cloud Computing and Virtualization Security Curve. Website of Cloud Security Alliance. – P. 1–6. URL: https://cloudsecurityalliance.org/wp- content/uploads/2011/ 11/DataCentricProtection_intheCloud.pdf

14. Berdnik, A.V. (2013). Problemy bezopasnosti oblachnykh vychislenii. Analiz metodov zashchity oblakov ot cloud security alliance. [Cloud computing security issues. Analysis of cloud protection methods from cloud security alliance]. Almanakh sovremennoi nauki i obrazovaniia. V: Almanakh sovremennoi nauki i obrazovaniia. – Tambov: Gramota. № 10. – S. 35–38. [in Russian]

15. Lubacz, J., Mazurczyk, W., Szczypiorski, K. (2014). Principles and Overview of Network Steganography. Communications Magazine. IEEE. V. 52. # 5. – P. 225–229. URL: http://arxiv.org/pdf/1207.0917.pdf

16. Bishop, M. (2004). Introduction to Computer Security, 1st ed. Boston: Pearson Education. –747p.

17. Prescott, E. Small (2011). Defense in Depth: An Impractical Strategy for a Cyber World. SANS Institute. – P. 2 – 4. URL: https://www.sans.org/reading- room/whitepapers/assurance/defense-depth-impractical-strategy-cyber-world-33896

18. Rzhaby, V. (2015).Yzbav'tes' ot opasenyy otnosytel'no bezopasnosty dannikh v oblake. [Get rid of concerns about data security in the cloud]. IBM developer Works. – 16 p. URL: https://www.ibm.com/developerworks/ru/library/dm-1408datasecuritycloud/dm-1408datasecuritycloud-pdf.pdf [in Russian]

19. Avoiding the hidden Costs of the Cloud: report of Symantec Corporation. (2013). – P. 1–11. URL: www.symantec.com/content/en/us/about/media/pdfs/b-state-of-cloud-global- results-2013.en-us.pdf

20. The Challenges of Cloud Information Governance: A Global Data Security Study: Ponemon Institute Research Report. (2014). P. 1–30. URL: http://www2.safenet- inc.com/cloud-security-research/SafeNet-Cloud-Governance.pdf

21. Sultan, N. (2014). Making use of cloud computing for healthcare provision: Opportunities and challenges. International Journal of Information Management. V. 34. – P. 177–184.

22. Hoff, Ch. (2011). In: Security guidance for critical areas of focus in cloud computing. – P. 12–20. URL: https://cloudsecurityalliance.org/ guidance/csaguide.v3.0.pdf

РЕФЕРАТ

Червякова Т.І. Інформаційна безпека технології хмарних обчислень. / Т.І. Червякова // Вісник Національного транспортного університету. Серія «Технічні науки». Науково-технічний збірник. – К.: НТУ, 2020. – Вип. 1 (46).

Стаття присвячена аналізу теоретичних і практичних аспектів технології хмарних обчислень, виявленню основних проблем забезпечення інформаційної безпеки різних моделей хмарних сервісів і моделей розгортання хмарного середовища, а також вибору методів забезпечення безпеки обробки даних і способів підвищення безпеки хмарних обчислень.

Об’єкт дослідження – інформаційна безпека технології хмарних обчислень.

Мета роботи – аналіз теоретичних і практичних аспектів інформаційної безпеки технології хмарних обчислень, визначення їх принципів і перспектив.

Методи дослідження – аналіз, синтез, узагальнення, систематизація, графічні.

Одним із основних підходів до реалізації хмарної інфраструктури є технологія віртуалізації – надання обчислювальних ресурсів, абстрагованих від їх реальної апаратної реалізації. Зі збільшенням ступеня відкритості технології хмарних обчислень, гнучкості роботи з нею й універсальності доступу зменшується захищеність системи і ускладняється методика забезпечення її безпеки.

Система хмарних обчислень може піддаватися декільком видам загроз безпеки, включаючи загрози цілісності, конфіденційності та доступності її ресурсів, даних і віртуальної інфраструктури.

При побудові системи інформаційної безпеки хмарного середовища слід враховувати модель його розгортання (приватна, публічна, суспільна чи гібридна хмара) та відмінності в шарах контролю і доступу користувача та провайдера в різних моделях хмарних сервісів (IaaS, PaaS, SaaS).

Найбільш ефективним і при цьому універсальним способом забезпечення в хмарі захисту даних, їх конфіденційності та цілісності – це використанням шифрування даних на рівні файлів при їх передачі по інформаційних мережах і при зберіганні всередині хмари.

IT-адміністратори і користувачі можуть частково повернути собі контроль над забезпеченням безпеки своїх даних, використовуючи рішення захисту, засновані на шифруванні даних. Використання відповідних методів шифрування запобігає неавторизованому доступу до даних незалежно від того, де вони знаходяться – в процесі передачі або зберігання в хмарі, і дозволяють організаціям використовувати переваги хмарних обчислень, не піддаючи важливі дані ризику або зводячи цей ризик до мінімуму.

КЛЮЧОВІ СЛОВА: ХМАРНІ ОБЧИСЛЕННЯ, ХМАРНІ СЕРВІСИ, ІНФОРМАЦІЙНА БЕЗПЕКА.

ABSTRACT

Cherviakova T.I. Information security of cloud computing technology. Visnyk National Transport University. Series «Technical sciences». Scientific and Technical Collection. – Kyiv: National Transport University, 2020. – Issue 1 (46).

The article is devoted to the analysis of theoretical and practical aspects of technology of cloud computing, revealing of the main problems of providing information security of various models of cloud services and models of deployment of cloud environments, as well as the choice of methods for providing security of data processing and methods for improving the safety of cloud computing.

Object of research – information security technology cloud computing.

The purpose of the work is to analyze the theoretical and practical aspects of information security technology of cloud computing, determination of their principles and perspectives.

Methods of research – analysis, synthesis, generalization, systematization, graphic.

One of the main approaches to the implementation of cloud infrastructure is the virtualization technology - the provision of computing resources abstracted from their real hardware implementation. With the increase in the degree of cloud computing technology openness, the flexibility of its operation and the universality of access, the security of the system decreases and requires more complicated methods of ensuring its security.

The cloud computing system can be exposed to several types of security threats, including threats to the integrity, privacy and availability of its resources, data, and virtual infrastructure.

The construction of the cloud computing security system requires taking into account the model of its deployment (private, public or hybrid cloud) and the differences in the levels of control and access for user and provider in different cloud service models (IaaS, PaaS, SaaS).

The most effective and thus universal way of ensuring data protection in the cloud, as well as its confidentiality and integrity, is to use the data encryption at the file level when transmitting over information networks and when storing inside the cloud.

IT-administrators and users can partially regain control over the security of their data, using security-based solutions based on data encryption. Using the appropriate encryption methods prevents unauthorized access to data, regardless of where they are located, in the process of transmitting or storing it in the cloud, and allowing organizations to take advantage of cloud computing without compromising or minimizing risk.

KEYWORDS: CLOUD COMPUTING, CLOUD SERVICES, INFORMATION SECURITY.

РЕФЕРАТ

Червякова Т.И. Информационная безопасность технологии облачных вычислений. / Т.И. Червякова // Вестник Национального транспортного университета. Серия «Технические науки». Научно-технический сборник. – К.: НТУ, 2020. – Вып. 1 (46).

Статья посвящена анализу теоретических и практических аспектов технологии облачных вычислений, выявлению основных проблем обеспечения информационной безопасности различных моделей облачных сервисов и моделей развертывания облачного среды, а также выбора методов обеспечения безопасности обработки данных и способов повышения безопасности облачных вычислений.

Объект исследования – информационная безопасность технологии облачных вычислений.

Цель работы – анализ теоретических и практических аспектов информационной безопасности технологии облачных вычислений, определение их принципов и перспектив.

Методы исследования – анализ, синтез, обобщение, систематизация, графические.

Одним из основных подходов к реализации облачной инфраструктуры является технология виртуализации – предоставление вычислительных ресурсов, отвлеченных от их реальной аппаратной реализации. С увеличением степени открытости технологии облачных вычислений, гибкости работы с ней и универсальности доступа уменьшается защищенность системы и осложняется методика обеспечения ее безопасности.

Система облачных вычислений может подвергаться нескольким видам угроз безопасности, включая угрозы целостности, конфиденциальности и доступности ее ресурсов, данных и виртуальной инфраструктуры.

При построении системы информационной безопасности облачной среды следует учитывать модель ее развертывания (частное, публичное, общественное или гибридное облако) и различия в слоях контроля и доступа пользователя и провайдера в различных моделях облачных сервисов (IaaS, PaaS, SaaS).

Наиболее эффективным и при этом универсальным способом обеспечения в облаке защиты данных, их конфиденциальности и целостности – это использованием шифрования данных на уровне файлов при их передаче по информационным сетям и при хранении внутри облака.

IT-администраторы и пользователи могут частично вернуть себе контроль над обеспечением безопасности своих данных, используя решения защиты, основанные на шифровании данных. Использование соответствующих методов шифрования предотвращает несанкционированный доступ к данным независимо от того, где они находятся – в процессе передачи или хранения в облаке, и позволяют организациям использовать преимущества облачных вычислений, не подвергая важные данные риску или сводя этот риск к минимуму.

КЛЮЧЕВЫЕ СЛОВА: ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ, ОБЛАЧНЫЕ СЕРВИСЫ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ.

АВТОР

Червякова Тетяна Іванівна, Національний транспортний університет, кандидат технічних наук, доцент кафедри електроніки та обчислювальної техніки, e https://orcid.org/0000-0002-3672-9173, e-mail: Cherviakova_T@mail.ru, тел.: +380674450896.

AUTHOR

Cherviakova Tatiana I., National Transport University, Ph.D., Associate Professor, Department of electronics and computers, https://orcid.org/0000-0002-3672-9173, e-mail: Cherviakova_T@mail.ru, tel.: +380674450896.

АВТОР

Червякова Татьяна Ивановна, Национальный транспортный университет, кандидат технических наук, доцент кафедры электроники и вычислительной техники, https://orcid.org/0000-0002-3672-9173, e-mail: Cherviakova_T@mail.ru, тел.: +380674450896.

РЕЦЕНЗЕНТИ:

Воркут Т.А., доктор технічних наук, професор, завідувач кафедри транспортного права та логістики Національного транспортного університету, м. Київ, Україна.

Івохін Є.В., доктор фізико-математичних наук, професор, професор кафедри системного аналізу та теорії прийняття рішень факультету комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка.

REVIEWERS:

Vorkut T.A., PhD, Professor, Head of Department of Logistics and Transport Law, National Transport University, Kyiv, Ukraine.

Ivohin E.V., PhD, Professor of Department of System Analysis and Decision-Making Theory, Faculty of Computer Science and Cybernetics, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.