DOI: https://doi.org/10.33216/2222-3428-2021-20-11

УДК 004.056

Рязанцев О.І., Кардашук В.С., Сафонова С.О., Рязанцев А.О.

ІНФОРМАЦІЙНО-ОРІЄНТОВАНИЙ ПІДХІД ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ У ХМАРНОМУ СЕРЕДОВИЩІ

У статті розглянуто інформаційно-орієнтований підхід забезпечення безпеки даних у хмарному середовищі. Виконано дослідження традиційних методів забезпечення безпеки у хмарному середовищі, існуючих концепцій, характеристик та критеріїв підходу для досягнення максимальної ефективності. Розроблено концептуальні основи інформаційно-орієнтованого підходу забезпечення безпеки даних у хмарному середовищі. Досліджено та обрано алгоритм шифрування та підтримки цілісності даних, алгоритм забезпечення контролю доступу та перевірки аутентифікації. Розроблено складову частину інформаційно-орієнтовного підходу, програму тестування клієнт-серверної моделі, що імітує хмарне середовище.

Результати проведених операцій показують, що запропоноване рішення є простим і не вимагає складних операцій. Крім того, накладні витрати на зберігання при створенні файлу ОБІ є низькими в порівнянні з наданими функціями. Цими функціями є: створення ОБІ-файлу з можливостями пошуку, політикою прихованого контролю доступу та цілісністю і достовірністю, незалежно від того, де він зберігається в хмарі. Запропоноване рішення може бути практично реалізовано з мінімальними витратами на обчислення і зберігання та є ефективним, так як воно не вимагає складних методів розподілення ключів і файл даних не потрібно шифрувати більше одного разу.

Для шифрування вихідного файлу на стороні власника даних, а потім для його дешифрування на стороні користувача використано програмне забезпечення AES Crypto.

Запропоноване рішення використовує криптосистему з публічним ключем для безпечного обміну даними захищених користувачів, що зберігаються в середовищі хмарних обчислень серед авторизованих користувачів. Ресурсом може бути набір даних або файл, який містить дані будь-якого типу, в тому числі текст, аудіо, зображення або відео. Для поширення секретного ключа для авторизованих користувачів, його зашифровано з використанням методу публічного шифрування відкритого ключа користувача.

Ключові слова: *хмарне середовище, інформаційно-орієнтована безпека даних, контроль доступу, перевірка цілісності, автентичність.*

Актуальність дослідження новітніх методів забезпечення безпеки в хмарному середовищі зумовлено тим, що при розповсюдженні цієї технології в корпоративному сегменті у споживачів виникає низка перешкод, що насамперед включає проблеми безпеки та конфіденційності. На додаток до традиційних ризиків безпеки, що виникають в обчислювальних системах, підключених до Інтернету, хмарні системи мають специфічні проблеми безпеки та конфіденційності через віртуалізацію хмар та характер своєї багаторівневої природи [1].

Постановка проблеми. Безпека – це одна спільна проблема для підприємств, що замислюються над впровадженням програмного забезпечення як послуги (SaaS - Software as a Service). Щоразу, коли конфіденційні дані компанії та бізнес-процеси доручаються стороннім постачальникам послуг, такі питання, як управління особистістю та доступом, повинні вирішуватися. Підприємства також повинні враховувати норми дотримання правил, які притаманні зберіганню даних клієнтів у віддаленому центрі обробки даних.

У послугах хмарних обчислень клієнти стурбовані переміщенням своїх конфіденційних даних і додатків зі своїх приватних обчислювальних середовищ в хмарне середовище, яке спільно використовується різними клієнтами і яке, зазвичай, доступне через загальнодоступну мережу. Опитування, проведене у вересні 2016 року Міжнародною корпорацією даних (IDC), показує кілька проблем, які стосуються клієнтів хмарних обчислень. За результатами дослідження, безпека (87,5 %), визначається як найвища проблема [2]. Проблеми безпеки в хмарних обчисленнях зазвичай пов’язані з основними технологічними компонентами, на які покладаються хмарні обчислення. Цими компонентами є [3]:

− веб-додатки та служби, що найбільш часто використовуються технологіями для доступу до хмарних обчислень.

− віртуалізація є основною технологією надання хмарних обчислень. Обидві SaaS і PaaS (платформа як послуга) засновані на віртуалізації інфраструктури, що надається на рівні IaaS (інфраструктурою як сервіс).

− криптографічні методи в даний час є найбільш поширеними методами для досягнення задовільного рівня вимог безпеки для хмарних обчислень.

Аналіз останніх досліджень і публікацій. Програмне забезпечення SaaS – модель розповсюдження програмного забезпечення, в якій сторонній постачальник розміщує програми та робить їх доступними для клієнтів через Інтернет [4]. SaaS – одна з трьох основних категорій хмарних обчислень, поряд з IaaS і платформою PaaS. Варіанти розміщення програмних продуктів у хмарних ресурсах – офісні додатки, СУБД, корпоративна пошта, ERP-системи, CRM-системи, документообіг та інші рішення тощо.

Метою статті є підвищення ефективності безпеки даних у хмарному середовищі. Об’єкт дослідження – хмарні середовища. Предмет дослідження – методи захисту даних у хмарних середовищах. Методи дослідження

– аналіз існуючих традиційних підходів методів захисту веб-сервісів та концептуальних складових інформаційної безпеки. При формалізації задачі дослідження використано модель SaaS.

Вирішення проблеми. Дослідження безпеки захисту даних у хмарних середовищах полягає в розроблені рішення, яке робить оригінальний дослідницький внесок в концепцію ОБІ, що вважається адекватним підходом до вирішення питань безпеки та конфіденційності в хмарних обчисленнях [5]. SaaS - це природна придатність для підприємств, які мають намір скоротити витрати на інформаційні технології (IT). В середньому фірми, які переходять на програмне забезпечення (ПЗ) SaaS з передплатників із встановлення великої капітальної інфраструктури, технічного обслуговування та модернізації, користуються зниженням витрат на IT більш ніж на 15 %, згідно з даними, зібраними компанією Computer World [6]. SaaS особливо добре підходить для малого бізнесу. Замість того, щоб вкладати кошти в додаткові потужності власного сервера та ліцензії на програмне забезпечення, компанії просто можуть щомісяця коригувати своє ПЗ як підписку на послугу, збільшуючи вимоги споживання вгору та вниз, виходячи з потреб проекту та інших змінних. Також збільшується пропускна здатність людини: IT-співробітники компанії звільняються від завдань, пов'язаних з локальним обладнанням та ПЗ, що дозволяє їм вирішувати проекти, які є більш важливими для майбутнього зростання компанії. Оскільки IT-інфраструктура знаходиться в центрі даних постачальника послуг, організація може негайно відновитись і запуститись у разі відключення послуги або більш різкого збою.

Звичайно, ніщо не є ідеальним, і SaaS не є винятком. Компанії, які приймають кілька службових програм як ПЗ або планують підключити розміщене ПЗ до існуючих локальних програм, можуть зіткнутися з проблемами інтеграції програм [7]. Отже, будь-які відомі вразливості вищезазначених трьох основних технологічних компонентів можна розглядати як вразливості хмарних обчислювальних систем (ОС). Наприклад, протокол HTTP, який використовується в веб-технологіях, піддається перехопленню сеансів та атакам сеансового рівня. Тому хмарні ОС вразливі для такого роду атак і повинні подолати цю слабкість. Віртуалізація - ще одна вразлива проблема. Зловмисник може прорватися через віртуальний «бар'єр» і отримати доступ до даних і ресурсів або пасивно, спостерігаючи за даними, або активно, змінюючи дані і конфігурації. Крім того, існують різні інші можливі вразливості, які можуть бути присутніми в хмарних ОС, і вони пов'язані з його інфраструктурою та середовищем. Оскільки хмарні послуги, зазвичай, надаються через Інтернет, всі очікувані проблеми, пов'язані з Інтернетом, також пов'язані з хмарними обчисленнями. Вразливості в ОС і інших програмах, реалізованих програмно і встановлених в хмарну інфраструктуру, також можна розглядати як такі, що пов'язані з уразливостями хмарних обчислень [8].

Несанкціонований доступ до інтерфейсу управління: в хмарних обчисленнях інтерфейси управління зазвичай доступні через загальнодоступні мережі для авторизованих клієнтів і можливих неавторизованих зловмисників, тоді як звичайні центри обробки даних зазвичай доступні тільки авторизованим адміністраторам безпосередньо або через приватні мережі. Більш того, доступ до управління зазвичай здійснюється через веб-додаток або сервісні технології, тому інтерфейс управління хмарами, ймовірно, схильний до вразливості цих технологій.

Проблема відновлення даних: через природу віртуалізації і спільного використання хмарних послуг на апаратному рівні області пам'яті і зберігання, які були орендовані попередніми клієнтами, можуть бути перерозподілені для нових клієнтів. Можливо, що ці нові клієнти можуть відновлювати дані з цих областей пам'яті і зберігання, які можуть містити конфіденційну інформацію, що належить попереднім клієнтам.

Вразливість образу шаблону віртуальної машини (VM): нова віртуальна машина зазвичай створюється шляхом клонування образу шаблону попередньо сконфігурованої віртуальної машини, так як це економить час і зусилля. Таким чином, багато клієнтів будуть орендувати віртуальні машини з однаковими конфігураціями. Зловмисник може збирати інформацію про образи шаблонів хмарних систем, ставши клієнтом хмари з правами адміністратора. Як тільки зловмисник має доступ до образів шаблонів, він може шукати вразливості в цих образах, які також використовуються іншими клієнтами.

Можливість витоку даних: інша проблема вразливості, пов'язана з образами шаблонів віртуальних машин, полягає в тому, що хмарні провайдери можуть використовувати шаблони, створені іншими клієнтами для нових клієнтів. Ці шаблони можуть містити секретні бекдори, створені зловмисником, що прикидатися клієнтом, і дозволяють зловмисникові отримати доступ до віртуальних машин інших клієнтів.

Ін'єкційні вразливості: оскільки більшість хмарних сервісів використовують служби веб-додатків, можна вводити зловмисні коди в хмарну систему, використовуючи вразливості в таких службах веб-додатків, щоб зламати веб-сервери, які обслуговують ці служби. Існує багато прикладів способів злому з використанням зловмисних кодів, таких як коди SQL, команда ОС або коди JavaScript. Як тільки веб-сервер зламаний, він може використовуватися в якості стартового майданчика для зловмисника для зломуя інших цілей в системі, і ці цілі включають бази даних і операційні системи.

Метрики безпеки і труднощі моніторингу: клієнти повинні мати можливість вимірювати і контролювати ситуацію безпеки своїх хмарних послуг і ресурсів. Однак надання таких можливостей хмарним клієнтам як і раніше є проблемою, тому що доступні традиційні стандартні інструменти ще не підходять для хмарного середовища. Оскільки хмарне середовище має складні і динамічні ієрархічні сервіси, які можуть включати в себе різних провайдерів хмарних обчислень, хмарне середовище вимагає нових розподілених можливостей моніторингу, відповідних цим характеристикам.

Складність в управлінні цифровими ключами і випадковими числами: в хмарній системі існують різні типи ключів і випадкових чисел, необхідні для криптографічних операцій. Управління та зберігання різних ключів в

хмарному середовищі - непрості завдання, тому що немає повної фізичної ізоляції між ресурсами зберігання, виділеними для різних клієнтів. Ефективність генерації випадкових чисел в основному залежить від апаратного годинника, використовуваного генератором випадкових чисел. Відсутність такої ефективності може бути випробувано в хмарному середовищі, де в різних сеансах кілька хмарних клієнтів використовують одні і ті ж ресурси генерації одночасно. Це може призвести до перевантаження ресурсів генерації випадкових чисел, або може привести до отримання слабких чисел. Таким чином, впровадження стандартних механізмів безпеки, таких як модуль апаратної безпеки, який спирається на ефективний ресурс генерації випадкових чисел, в хмарні системи є проблемою безпеки.

Проблема функціональної сумісності хмари: ця проблема пов'язана з тим, як різні хмарні провайдери дозволяють власникам даних безперешкодно переміщати свої дані від одного провайдера до іншого або від хмарного провайдера назад в свої локальні ресурси, коли їм це потрібно. Без функціональної сумісності між хмарними провайдерами, власник даних може заблокувати певного провайдера і не зможе легко перейти до інших провайдерів або оптимізувати послуги між різними провайдерами.

Спостереження за шаблонами активності: шаблони активності одного хмарного клієнта можуть спостерігатися або іншими клієнтами в одній хмарі, або хмарним провайдером. Це спостереження може бути кроком для атаки безпеки або може бути використано для виявлення ділових дій, які не можуть бути виявлені в звичайних обставинах. Наприклад, обмін інформацією між двома компаніями може свідчити про планування злиття. Необхідність взаємних можливостей проведення аудиту, підзвітності і надійність: довіра повинна будуватися між провайдерами і клієнтами в хмарному середовищі. Прозорість через високий рівень можливостей проведення аудиту і підзвітності має важливе значення для створення довірливих відносин. Довірливі відносини будуть більш складними, якщо хмарні провайдери делегують деякі з хмарних сервісів субконтрактам. Клієнти хмарних обчислень повинні знати, чи є які-небудь субконтракти, які також можуть відповідати за їх дані і додатки за хмарою. Наприклад, Linkup надав онлайн-службу зберігання через іншого субпідрядного провайдера під назвою Nirvanix, перш ніж він закрився в результаті втрати значної кількості клієнтських даних. Ймовірно, субпідрядник ніс відповідальність за втрату клієнтських даних.

Тенденції та напрямки рішень. Технологія хмарних обчислень стикається з різними проблемами, які не можна вирішувати безпосередньо традиційними рішеннями. Відповідне рішення має бути адаптоване до конкретних характеристик цієї нової обчислювальної парадигми. Дослідницькі напрямки вирішення проблем хмарних обчислень різні в залежності від того, на яких видах хмарних проблем зосереджуються дослідники. На рівні віртуалізації технології стверджується, що проблеми, пов'язані з ізолюванням віртуальних машин на одній фізичній машині, вимагають більшої уваги з точки зору безпеки та продуктивності. Для більш високого рівня важливості, з приводу складнощів довіри у розрахунку на багато клієнтів і вимог до можливостей взаємного аудиту в хмарних обчисленнях, можуть стати новими важливими завданнями. Проте, можна стверджувати, що конфіденційність і цілісність даних є основною вимогою безпеки, особливо в ненадійних хмарах. Також в надійних або частково надійних хмарах сильним механізмом конфіденційності може бути ключ до встановлення надійності. Ненадійний сервер хмарних обчислень може надавати персональні дані і шаблони активності клієнтів і повертати невірні дані від обчислювальних процесів клієнтам. Також можливо, що ненадійний провайдер може маніпулювати законним способом обробкою запитів користувачів в їх інтересах. Таким чином, захист даних, зокрема їх конфіденційності і цілісності, як від провайдерів хмарних послуг, так і від зовнішніх зловмисників, як очікується, призведе до створення більш сильних архітектур безпеки хмар, які сприятимуть ширшому впровадженню хмарних сервісів.

У хмарних обчисленнях дані користувачів, в основному, зберігаються у віртуальних сховищах провайдерів хмарної інфраструктури. В публічних SaaS та DaaS моделях користувачі володіють лише даними, які знаходяться на зберіганні. Все обладнання та програмне забезпечення, залучене до зберігання та обробки інформації, знаходиться у власності сервіс провайдерів. В інших моделях, таких як публічні IaaS и PaaS моделі, користувач має доступ до обробки даних та до програмного забезпечення, при цьому доступу до апаратного забезпечення немає.

У даній роботі, з точки зору розуміння концепції ОБІ, існуючі рішення можуть бути класифіковані за двома критеріями:

– класифікація заснована на тому, на якому рівні забезпечується безпека;

– класифікація на тому, хто несе відповідальність за забезпечення безпеки.

На правій частині рисунку 1, проілюстровано рівні які можуть бути передбачені функцію безпеки по відношенню до даних. В цілому, рішення сфокусоване на забезпечення безпеки поза рівнем даних класифікуються як системно-центровані. Якщо рішення сфокусовано на окремому визначеному рівні, його класифіковано відповідно до цього специфічного рівня. Наприклад, рішення спрямовані на поліпшення безпечної ізоляції між віртуальною машиною та гіпервізором можуть бути класифіковані як VM-орієнтовані рішення в області безпеки. З іншого боку, рішення, спрямовані на забезпечення безпеки даних усередині самих даних, як показано на лівій частині рисунку 1, класифікуються як інформаційно-орієнтовані підходи.

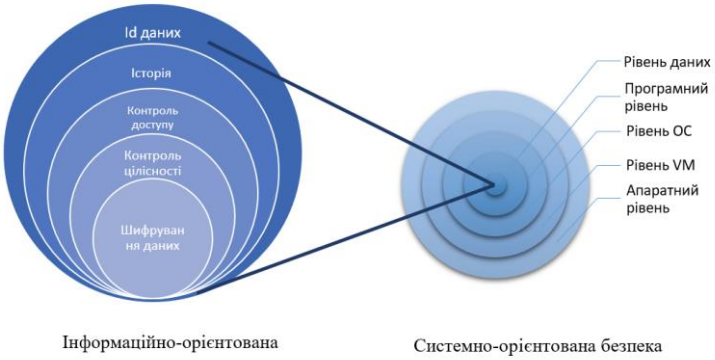

Рисунок 1 – Інформаційно-орієнтована та системно-орієнтована моделі

Рівні, показані на рисунку 1, є типовими рівнями. Там може бути більше або менше рівнів в практичній системі, на основі фактичних потреб та реалізації.

Приклад другої класифікації показано на рисунку2.

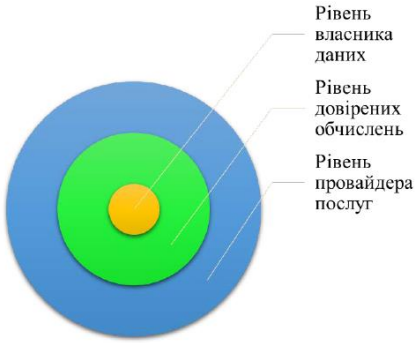

Рисунок 2 – Можливі рівні безпеки

Існує три рівні відповідальності безпеки:

− рівень сервіс провайдерів, де забезпечується безпека та здійснюється підтримка хмарних провайдерів;

− рівень довірених обчислень, де забезпечується безпека та організатором виступає третя сторона;

− рівень даних, на якому забезпечується безпека та організаторами виступають власники даних.

На даний момент концепція ОБІ (орієнтація на безпеку інформації) знаходиться на етапі зародження, проте стрімко розвивається. Систематичний перегляд літератури в напрямку пошуку реалізованих систем інформаційно-орієнтованої безпеки не дало плідних результатів. Проте можна відзначити роботу колег з Індії, які практично дослідили інформаційно-орієнтовану систему безпеки на прикладі розподіленої системи охорони здоров'я. Значність результатів дослідження підкріплюється авторитетом міжнародної конференції «Розподілених обчислень та мереж».

Власник даних зазвичай є найкращим суб'єктом для оцінки вимог безпеки своїх власних даних. Наприклад, якщо дані підключені до бізнес-моделі, вимоги до безпеки даних повинні бути результатом аналізу їх використання в бізнес-процесі. Як правило, дані повинні оброблятися відповідно до їх значенням, оскільки наступний принцип безпеки проголошує: «цінність того, що захищається, впливає на заходи, прийняті для його захисту». Отже, дані класифікуються на основі оцінки власника даних та вимог до безпеки. Наприклад, дані можуть бути просто класифіковані як цілком таємні, секретні або конфіденційні. Виходячи з цього, політики контролю доступу та властивості безпеки, необхідні для обробки даних, надаються відповідно до цих вимог безпеки. Класифікація даних на концептуальному рівні може бути представлена як інформація, приєднана до даних, або представлена на вимогу необхідних заходів безпеки, які застосовуються до даних.

Параметри контролю доступу приховані від провайдерів хмарних серверів та інших користувачів. Провайдер серверу не знає кількість або особистість користувачів, що авторизовані та мають право доступу до даних.

Несанкціоновані об'єкти, в тому числі постачальники послуг, не можуть отримати доступ до даних або отримати інформацію про дані від авторизованих процесів що проводяться на даних. Дані містять всю необхідну інформацію для перевірки їх цілісності для авторизованих користувачів, які мають доступ до даних.

Взаємодія між власниками та авторизованими користувачами має бути мінімальною, особливо щодо ключових цілей управління. Ці вимоги визначені набором модулів, кожен з яких точно описаний принаймні однією із зазначених вище вимог. Всі параметри, необхідні для досягнення функцій безпеки прикріплюються до

файлу даних і в результаті є файл з назвою ОБІ-файл. Функції безпеки включають у себе захист конфіденційності, перевірку цілісності та аутентифікацію.

Інструменти реалізації і середовище експерименту. Засоби реалізації і середовище експерименту були підготовлені для сервера і клієнтської сторони. Для реалізації дослідження використано мову C#, що базується на Eclipse IDE. Віртуальна серверна платформа, що представляє хмарний сервер, була встановлена на персональному комп'ютері з наступними характеристиками:

– процесор: i5-7400 3.0GHz/8GT/s/6MB;
– оперативна пам’ять: 16 ГБ;
– загальна сховище на жорсткому диску: 256 ГБ (SSD).

Для створення віртуального сервера використана платформа VMware VSphere 6.

VMware є одним зі світових лідерів в області віртуалізації і хмарної інфраструктури. Віртуальний сервер був налаштований з такими специфікаціями:

– ОС: Windows Server 2019 Enterprise 64-розядної версії;
– віртуальна пам’ять: 8 ГБ;
– віртуальний простір для зберігання: 100 ГБ;
– процесор: 2 ядра Intel i5-7400 3.0 ГГц.

Інші віртуальні машини були встановлені на тому ж виділеному апаратному сервері для створення віртуального середовища, що імітує середу віртуалізації, яка використовується в публічній хмарі.

В публічній хмарі кілька клієнтів використовують один і той же апаратний сервер, використовуючи свої віртуальні машини, що працюють на одному і тому ж апаратному сервері. Ці віртуальні машини ізольовані віртуально з використанням платформи віртуалізації.

В експерименті використовувався комп’ютер з наступними характеристиками:

– процесор: Intel CORE i7 CPU 2.8 ГГц;
– пам’ять: 16 ГБ;
– ОС: Windows 10, 64 біт.

Комп’ютер використовувався для моделювання як сторони власника даних, так і авторизованого з користувальницького боку. З боку власника даних реалізовано і протестовано операції зі створення ОБІ-файлу перед його аутсорсингом на хмарний сервер. Для авторизованого користувача реалізація та тестування проводилися для операцій шляхом обчислення значення Cr||Ks із загального значення Xr, використовуючи рівняння (3.4), і шляхом дешифрування даних з файлу ОБІ, що містить зашифровані дані. На стороні сервера було виконано пошук ключових слів у ОБІ-файлі.

На рисунку 2 показано налаштування середовища експерименту, повідомлень, переданих між об’єктами, і основних операцій з кожного боку. На етапі реалізації одним із завдань був вимір службових даних сховища і накладних витрат на обчислення для виконання операцій ОБІ.

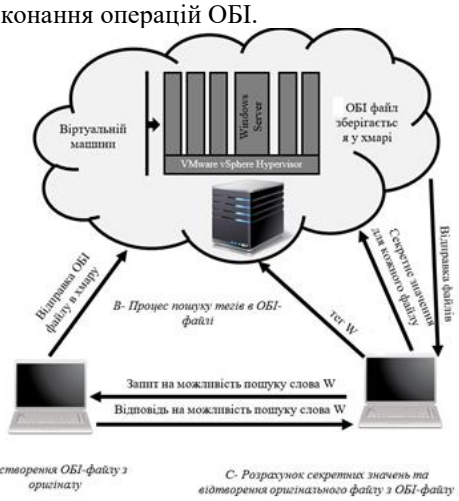

Рисунок 2 – Експериментальне середовище для запропонованого рішення

Реалізація програми на стороні клієнта. Клієнтська сторона може бути власником даних або авторизованим користувачем. Багато функцій, такі як асиметричний алгоритм шифрування, алгоритм симетричного шифрування та обчислення хеша файлу, використовуються як власником даних, так і авторизованим користувачем. Пошук рішення і шифрування ключових слів виконується тільки власником даних.

Симетричне шифрування вихідного файлу. Шифрування даних за допомогою симетричного алгоритму шифрування є найбільш важливою операцією. Для надійного захисту дані повинні бути зашифровані, навіть якщо вони залишаться у власності власника даних. Тому перша дія після класифікації даних як конфіденційних даних – це шифрування даних з використанням адекватного алгоритму шифрування і сили ключа. У загальному випадку алгоритм симетричного шифрування використовується замість асиметричного шифрування для шифрування великої кількості даних, оскільки він більш ефективний.

У даній реалізації файли зашифровуються за допомогою Advanced Encryption Standard (AES), що забезпечується програмою AES Crypt з відкритим вихідним кодом для платформ Windows з використанням 256-бітної довжини ключа, сильнішої довжини ключа для цього алгоритму.

Накладні витрати на зберігання складають близько 300 байт для всіх файлів. Збільшується обчислювальне навантаження зі збільшенням розміру файлу, щоб досягти більш ніж однієї хвилини для файлу з розміром 571 МБ. Ця операція є основою для будь-якого методу, заснованого на шифруванні даних, перш ніж дані будуть відправлені в хмару. Крім того, важливо вибрати сильний алгоритм шифрування і довший ключ для досягнення більш високої безпеки. Однак власники даних мають гнучкість, відповідно до їх вимог безпеки, щоб зменшити обчислювальні накладні витрати, використовуючи більш короткий ключ або слабший алгоритм шифрування з меншими обчислювальними витратами. Загалом, процес шифрування несе в собі найбільші обчислювальні витрати на стороні власника даних в запропонованому в цій роботі методі.

В таблиці 1 показані накладні витрати на зберігання і час виконання шифрування файлів різних типів даних з використанням алгоритму AES з розміром ключа 256 біт.

Таблиця 1 – Зберігання та часові накладні витрати для шифрування AES

Назва файлу	Розмір в байтах	Розмір після шифрування в байтах	Збільшення розміру в байтах	AES шифрування в секундах
Sample.docx	14,175	14,485	310	<1
visio.vsd	45,029	45,341	312	<l
photo.jpg	64,819	65,130	318	<1
video1.wmv	25,327,026	25,327,338	312	1.6
video2.mov	41,670,503	41,670,812	309	2.3
video3.avi	136,318,116	136,318,429	313	14.8
video4.mov	598,787,322	598,787,634	311	86.7

Обчислення рішення для визначення значення Xr є суттєвою частиною запропонованого рішення. На основі цієї цінності засновані політики обміну ключами і контролю доступу. На розрахунок КТЗ (китайська теорема про залишки) не впливає розмір файлу, але на нього впливає кількість користувачів і алгоритм асиметричного шифрування, використовуваний для шифрування значення *Cr||Ks*.

Витрати часу на зберігання і час при обчисленні КТЗ-рішення показані для різних користувачів з двох до шести. Ці обчислення виконувалися, коли значення Cr||Ks було зашифровано з 1024-бітовим RSA і кожне відносне просте число було 1022-бітним. Результати показують, що сама операція КТЗ вимагає незначного часу виконання. Наприклад, для шести користувачів обчислення КТЗ-рішення зайняло близько 6 мілісекунд. Час виконання обчислення значення обумовлено головним чином процесом шифрування КТЗ і збільшується зі збільшенням кількості користувачів. Однак, оскільки процес шифрування КТЗ виконується для фіксованого значення довжини Cr||Ks, загальний час виконання пошуку все ще незначний і задовільний. Наприклад, загальний час становив 31 мс для шести користувачів, а загальний час збільшувалася приблизно на 2 мс для кожного додаткового користувача. Більшість витрат, викликаних операцією КТЗ - це накладні витрати на зберігання, які збільшуються зі збільшенням числа користувачів.

В таблиці 2 наведені результати, щодо часових витрат на зберігання та розрахунку загального значення Xr

Таблиця 2 – Часові витрат на зберігання та розрахунку загального значення Xr

№ користувача	1024 біти шифрування для Cr||Ks в мс	Підрахунок рішення Xr в мс	Загальний час підрахунку Xr в мс	Довжина Xr в бітах
1	21	3	24	2049
2	22	4	26	3073
3	23	4	27	4097
4	24	5	29	5118
5	25	6	31	6142

На підставі результатів таблиці 2 розмір Xr лінійно збільшується приблизно на 1000 біт для кожного додаткового користувача, коли довжина ключа КТЗ дорівнює 1024 біти. Наприклад, для шести користувачів розмір дорівнює 6142 біт.

ВИСНОВКИ. Досліджені традиційні методи забезпечення безпеки у хмарному середовищі та існуючі концепції орієнтовані на безпеку інформації, визначені характеристики та критерії підходу для досягнення максимальної ефективності; розроблені концептуальні основи інформаційно-орієнтованого підходу; досліджено та обрано алгоритм шифрування даних та підтримки цілісності, алгоритм забезпечення контролю доступу та перевірки аутентифікації, розроблена складова частини інформаційно-орієнтовного підходу, що забезпечує безпечний пошук у зашифрованих даних, проведено тестування клієнт-серверної моделі, що імітує хмарне

середовище. Рішення призначене для задоволення переліку бажаних вимог до додатків в середовищі хмарних обчислень, які зашифровані та доступні лише для авторизованих користувачів, доступні для пошуку без загрози для їх конфіденційності, відповідають вимогам самозахисту та необхідним параметрам безпеки.

Література

1. Что такое модель SaaS, ее преимущества и примеры. [Електронний ресурс]. – Режим доступу: https://www.kasper.by/blog/model-saas/ (дата звернення 19.02.2021).
2. Платформа как услуга. [Електронний ресурс]. – Режим доступу: https://azure.microsoft.com/ru-ru/overview/what-is-paas/ (дата звернення 20.01.2021).
3. Хмарна піраміда: SaaS, PaaS, IaaS. [Електронний ресурс]. – Режим доступу: https://gigacloud.ua/blog/navchannja/hmarna-piramida-iaas-paas-i-saas (дата звернення 20.02.2021).
4. The SaaS Business Model Explained Greg Elfrink June 22, 2016. [Електронний ресурс]. – Режим доступу: https://empireflippers.com/saas-business-model-explained/ (дата звернення 24.02.2021).
5. Brian Mackley. SaaS 101: Starting a Software as a Service Business. [Електронний ресурс]. – Режим доступу: https://articles.bplans.com/software-as-a-service-or-saas-101/ (дата звернення 24.02.2021).
6. Базиленко Анна. Усі хмарні сервіси Google об'єднали під спільним брендом Google Cloud. [Електронний ресурс]. – Режим доступу: http://watcher.com.ua/2016/09/30/usi-hmarni-servisy-google-ob-yednaly-pid-spilnym-brendom-google-cloud/ (дата звернення 20.01.2021).
7. Сергій Депутат. Гігабайти в хмарі. Чотири кращих хмарних сервіса для зберігання даних. [Електронний ресурс]. – Режим доступу: https://techno.nv.ua/ukr/it-industry/hihabajti-v-khmari-chotiri-krashchikh-khmarnikh-servisu-dlja-zberihannja-danikh-2448855.html (дата звернення 20.02.2021).
8. Аулов І.Ф. Дослідження моделі загроз ключових систем хмари та пропозиції захисту від них. Східноєвропейський журнал передових технологій. 5/2 (77), 2015. С.4-13.
9. Популярні хмарні сервіси: особливості роботи та важливі налаштування. [Електронний ресурс]. – Режим доступу: http://gsm-ka.com.ua/ua/populyarnye-oblachnye-servisy-osobennosti-raboty-i-vazhnye-nastroyki/ (дата звернення 24.01.2021).

Reference

1. Shcho take model′ SaaS, yiyi perevahy ta pryklady. [Elektronnyy resurs]. - Rezhym dostupu: https://www.kasper.by/blog/model-saas/ (data Zvernennya 19.02.2021).
2. Platforma yak posluha. [Elektronnyy resurs]. - Rezhym dostupu: https://azure.microsoft.com/ru-ru/overview/what-is-paas/ (data Zvernennya 20.01.2021).
3. Sonyachno piramida: SaaS, PaaS, IaaS. [Elektronnyy resurs]. - Rezhym dostupu: https://gigacloud.ua/blog/navchannja/hmarna-piramida-iaas-paas-i-saas (data Zvernennya 20.02.2021).
4. The SaaS Business Model Explained Greg Elfrink June 22, 2016. [Elektronnyy resurs]. - Rezhym dostupu: https://empireflippers.com/saas-business-model-explained/ (data Zvernennya 24.02.2021).
5. Brian Mackley. SaaS 101: Starting a Software as a Service Business. [Elektronnyy resurs]. - Rezhym dostupu: https://articles.bplans.com/software-as-a-service-or-saas-101/ (data Zvernennya 24.02.2021).
6. Bazylenko Anna. Usi khmarni servisy Google ob'yednaly pid spil′nim brendom Google Cloud. [Elektronnyy resurs]. - Rezhym dostupu: http://watcher.com.ua/2016/09/30/usi-hmarni-servisy-google-ob-yednaly-pid-spilnym-brendom-google-cloud/ (data Zvernennya 20.01.2021).
7. Serhiy Deputat. Hihabayti v khmari. Chotyry krashchykh Sonyachno servisa dlya zberihannya Danykh. [Elektronnyy resurs]. - Rezhym dostupu: https://techno.nv.ua/ukr/it-industry/hihabajti-v-khmari-chotiri-krashchikh-khmarnikh-servisu-dlja-zberihannja-danikh-2448855.html (data Zvernennya 20.02.2021).
8. Aulov I.F. Doslidzhennya modeli zahroza klyuchovymy system khmary ta propozytsiyi zakhystu vid nykh. Skhidnoyevropeys′kiy zhurnal peredovykh tekhnolohiy. 5/2 (77), 2015. S.4-13.
9. Populyarni khmarni servisy: Osoblyvosti roboty ta Vazhlyvi nalashtuvannya. [Elektronnyy resurs]. - Rezhym dostupu: http://gsm-ka.com.ua/ua/populyarnye-oblachnye-servisy-osobennosti-raboty-i-vazhnye-nastroyki/ (data Zvernennya 24.10.2019).

В статье рассмотрен информационно-ориентированный подход обеспечения безопасности данных в облачной среде. Выполнены исследования традиционных методов обеспечения безопасности в облачной среде, существующих концепций, характеристик и критериев подхода для достижения максимальной эффективности. Разработаны концептуальные основы информационно-ориентированного подхода обеспечения безопасности данных в облачной среде. Исследован и избран алгоритм шифрования и поддержки целостности данных,

алгоритм обеспечения контроля доступа и проверки подлинности. Разработана составная часть информационно-ориентированного подхода, программу тестирования клиент-серверной модели, имитирующей облачную среду.

Результаты проведенных операций показывают, что предложенное решение является простым и не требует сложных операций. Кроме того, накладные расходы на хранение при создании файла ОБИ являются низкими по сравнению с предоставленными функциями. Этими функциями являются: создание ОБИ-файла с возможностями поиска, политикой скрытого контроля доступа и целостностью и достоверностью, независимо от того, где он хранится в облаке. Предложенное решение может быть практически реализовано с минимальными затратами на вычисления и хранения и является эффективным, так как оно не требует сложных методов распределения ключей и файл данных не требуется шифровать более одного раза.

Для шифрования исходного файла на стороне владельца данных, а затем для его дешифровки на стороне пользователя использовано программное обеспечение AES Crypto.

Предложенное решение использует криптосистему с публичным ключом для безопасного обмена данными защищенных пользователей, хранящихся в среде облачных вычислений среди авторизованных пользователей. Ресурсом может быть набор данных или файл, содержащий данные любого типа, в том числе текст, аудио, изображения или видео. Для распространения секретного ключа для авторизованных пользователей, его зашифровано с использованием метода публичного шифрования открытого ключа пользователя.

Ключевые слова: облачная среда, информационно-ориентированная безопасность данных, контроль доступа, проверка целостности, подлинность.

The relevance of the study of the latest methods of security in the cloud environment is due to the fact that the spread of this technology in the corporate segment of consumers has a number of obstacles, including security and privacy issues. In addition to the traditional security risks that arise in Internet-connected computing systems, cloud systems have specific security and privacy issues due to cloud virtualization and the nature of their multilevel nature.

The paper considers an information-oriented approach to data security in a cloud environment. Conducted research on traditional methods of security in a cloud environment, research on existing concepts focused on information security, defining the characteristics and criteria of the approach for maximum efficiency. Conceptual bases of information-oriented approach of data security in the cloud environment are developed. The algorithms of data encryption and data integrity support, algorithms for access control and authentication are investigated and selected.

An integral part of the information-oriented approach has been developed that provides secure search in encrypted data, a program for testing a client-server model that simulates a cloud environment.

Encrypting data using a symmetric encryption algorithm is the most important operation. For secure protection, data must be encrypted, even if it remains the property of the data owner. Therefore, the first step after classifying data as confidential data is to encrypt the data using an adequate encryption algorithm and key strength. In the general case, the symmetric encryption algorithm is used instead of asymmetric encryption to encrypt large amounts of data because it is more efficient.

In this implementation, the files are encrypted using the Advanced Encryption Standard (AES) provided by the open source AES Crypt program for Windows platforms using a 256-bit key length, the stronger key length for this algorithm.

Keywords: cloud environment, information-oriented data security, access control, integrity checking, authentication.

О.І. Рязанцев професор, завідувач кафедри комп’ютерних наук та інженерії Східноукраїнського національного університету ім. В. Даля.

В.С. Кардашук доцент кафедри комп’ютерних наук та інженерії Східноукраїнського національного університету ім. В. Даля.

С.О. Сафонова доцент кафедри комп’ютерних наук та інженерії Східноукраїнського національного університету ім. В. Даля.

А.О. Рязанцев аспірант кафедри комп’ютерних наук та інженерії Східноукраїнського національного університету ім. В. Даля.