Математичні методи, моделі та інформаційні технології в економіці

УДК 330.46

Камінський Олег Євгенович
кандидат економічних наук, доцент,
доцент кафедри інформаційного менеджменту
Київський національний економічний університет
імені Вадима Гетьмана
Каминский Олег Евгеньевич
кандидат экономических наук, доцент,
доцент кафедры информационного менеджмента
Киевский национальный экономический университет
имени Вадима Гетьмана
Kaminsky Oleg
PhD in Enterprise Economics, Associate Professor,
Associate Professor of Information Management Department
Kyiv National University of Economics named after Vadym Hetman

ОЦІНЮВАННЯ РИЗИКІВ БЕЗПЕКИ ХМАРНИХ СЕРВІСІВ
ОЦЕНКА РИСКОВ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СЕРВИСОВ
SECURITY RISK EVALUATION OF CLOUD SERVICES

Анотація. *Провайдери хмарних сервісів пропонують своїм клієнтам послуги з різними рівнями ризику безпеки. Користувачі хочуть мінімізувати даний ризик за певні витрати або інвестиції. Хмарні сервіси складаються з рівнів, які відповідають ієрархії хмари, тобто рівня програмного забезпечення, рівня платформи та рівня інфраструктури. Наразі хмарні провайдери надають сервіси у вигляді пакетів, які включають в себе програмне забезпечення, платформу та елементи інфраструктури. Хмарні технології служить альтернативою традиційної моделі локального*

використання апаратного та програмного забезпечення. У масштабах підприємства хмарні технології дозволять відмовитися від власної апаратно - програмної інфраструктури, замінивши її підключенням до відповідної мережевої послуги - хмари. Таким чином, парадигма хмарних обчислень здатна вплинути на розстановку сил на ринку як програмного, так і апаратного забезпечення. Метою статті є розробка теоретико-методологічних підходів до визначення суті та особливостей оцінювання ризиків безпеки хмарних сервісів, виявлення основних компонентів ризику на кожному рівні хмари, та розробка схеми обчислення консолідованого індикатора безпеки для хмарних сервісів. Запропонована модель оцінювання ризиків безпеки спрямована на потенційних клієнтів, які бажають порівняти ризики пакетів хмарних сервісів, що пропонуються різними хмарними провайдерами. У статті визначено основні фактори ризиків на кожному рівні хмари, їх типи та методи розрахунку та запропоновано схему для оцінки загального консолідованого індикатора безпеки хмарного сервісу. Запропонована модель дає можливість аналізувати ризики, що виникають під час упровадження конкретного хмарного сервісу або міграції до хмари всієї IT-інфраструктури підприємства, і на основі одержаних даних визначати важливість його створення або оренди.

Ключові слова: *інформаційні технології, хмарні обчислення, хмарні сервіси, моделі, управління ризиками, інформаційна безпека, хмарні платформи.*

Аннотация. *Провайдеры облачных сервисов предлагают своим клиентам услуги с разными уровнями риска безопасности. Пользователи хотят минимизировать данный риск, в обмен на определенные расходы или инвестиции. Облачные сервисы состоят из уровней, которые соответствуют иерархии облака, то есть уровня программного обеспечения, уровня платформы и уровня инфраструктуры. Сейчас*

облачные провайдеры предоставляют сервисы в виде пакетов, которые включают в себя программное обеспечение, платформу и элементы инфраструктуры. Облачные технологии служит альтернативой традиционной модели локального использования аппаратного и программного обеспечения. В масштабах предприятия облачные технологии позволят отказаться от собственной аппаратно-программной инфраструктуры, заменив ее подключением к соответствующей облачной услуге. Таким образом, парадигма облачных вычислений способна повлиять на расстановку сил на рынке как программного, так и аппаратного обеспечения. Целью статьи является разработка теоретико-методологических подходов к определению сущности и особенностей оценки рисков безопасности облачных сервисов, выявление основных компонентов риска на каждом уровне облака, и разработка схемы расчета консолидированного индикатора безопасности для облачных сервисов. Предложенная модель оценки рисков безопасности направлена на потенциальных клиентов, которые хотят сравнить риски пакетов облачных сервисов, предлагаемых различными облачными провайдерами. В статье определены основные факторы рисков на каждом уровне облака, их типы и методы расчета и предложена схема для оценки общего консолидированного индикатора безопасности облачного сервиса. Предложенная модель позволяет анализировать риски, возникающие при внедрении конкретного облачного сервиса или миграции в облака всей ИТ-инфраструктуры предприятия, и на основе полученных данных определять важность его создания или аренды.

Ключевые слова: *информационные технологии, облачные вычисления, облачные сервисы, модели, управления рисками, информационная безопасность, облачные платформы.*

Summary. *Cloud service providers offer their clients with different levels of security risk. Users want to minimize this risk for certain costs or investments. Cloud services consist of levels that correspond to the hierarchy of the cloud, namely, the level of software, level of platform level and level of infrastructure. Currently, cloud providers provide package services that include software, platform, and infrastructure elements. Cloud technologies serve as an alternative to the traditional model of local use of hardware and software. On a company-wide scale, cloud-based technologies will allow the abandonment of its own hardware-software infrastructure, replacing it with the connection to the corresponding network service - the cloud. Thus, the paradigm of cloud computing can affect the alignment of forces on the market, both software and hardware. The purpose of the article is to develop theoretical and methodological approaches to the definition of the essence and features of assessing the security risks of cloud services, to identify the main components of risk at each level of the cloud, and to develop a scheme for calculating the consolidated security indicator for cloud services. The proposed risk assessment model is aimed at potential customers who want to compare the risks of cloud service packages offered by different cloud providers. The article defines the main risk factors at each level of the cloud, their types and methods of calculation, and proposes a scheme for estimating the overall consolidated cloud service safety indicator. The proposed model provides an opportunity to analyze the risks arising from the implementation of a specific cloud service or migration to the cloud of the entire IT infrastructure of the enterprise and, based on the data obtained, determine the importance of its creation or lease.*

Key words: *information technologies, cloud computing, cloud services, models, risk management, information security, cloud platforms.*

Постановка проблеми. Традиційно, підприємства та організації розміщують свої обчислювальні потужності в центрах обробки даних, які

знаходяться всередині організації. Але останніми роками підприємства почали переносити частини свої IT-інфраструктури за межі власних офісів до хмар, де елементами інфраструктури володіють та управляють інші, спеціалізовані, компанії. Для цього керівники підприємств повинні розробити нові процеси контролю виробництва, моніторингу рівня обслуговування та вирішити питання безпеки та конфіденційності даних.

Національний інститут стандартів і технологій (NIST) визначає хмарні обчислення як модель для забезпечення зручного доступу до мережі об'єднаних в загальний пул обчислювальних ресурсів (наприклад, серверів, сховищ, програм і служб), який може бути швидко забезпечений з мінімальними управлінськими зусиллями через взаємодію сервіс-провайдер [1].

Хмарні обчислення орієнтовані на чотири основні групи підприємств -клієнтів: приватні, публічні, соціальні та гібридні [2]. Для приватних клієнтів IT-інфраструктура, як правило, розташована за межами організації у постачальника хмарних послуг. Публічні клієнти, як правило, обирають постачальників хмарних послуг через процедуру торгів, вибираючи найкращу пропозицію та підписуючи контракт з провайдером, що має найкращу пропозицію. Провайдери хмар можуть використовувати одну і ту ж обчислювальну інфраструктуру для забезпечення потреб кількох компаній. У соціальній моделі розгортання хмарна інфраструктура поділяється між групою користувачів соціальних мереж. У гібридній моделі розгортання організація може використовувати хмарні послуги, що надаються державними та приватними провайдерами хмар, або виступати як частина спільноти соціальної мережі. У роботі [3] досліджено появу нових тем у технологіях фінансових послуг і виявлено, що хмарні обчислення є економічно ефективною інфраструктурою, яка забезпечує ефективність капіталу для постачальників фінансових послуг.

Аналіз останніх досліджень та публікацій. Зарубіжні та вітчизняні дослідники вважають, що проблеми з безпекою є однією з найбільших перешкод на шляху до повного переходу на використання хмарних сервісів [4]. У дослідженні Т. Аккермана та інших [5] зазначено, що хмарні обчислення, як найпоширеніша парадигма IT-аутсорсингу все ще має серйозні ризики щодо IT-безпеки, а також стверджується, що дослідники все ще не в змозі повною мірою відобразити складний характер ризиків IT-безпеки та методи їх вимірювання. Аналітики дослідницької та консультаційної компанії в сфері промисловості IDC повідомляють, що 87,5% їх клієнтів вважають, що безпека хмари є головною проблемою [6]. В роботі дослідників С. Ядава та Д. Тіанксі [7] доведено, що управління ризиками безпеки для бізнес-систем стає дедалі складнішим і трудомістким, і багато наукових публікацій включають пропозиції, спрямовані на запобігання різним загрозам безпеці в мережі Інтернет.

Безпека хмари охоплює кілька категорій. В роботі Д. Фернандеса та Л. Соареса [8] були проаналізовані наукові публікації з проблем хмарної безпеки, що стосуються вразливостей, загроз та нападів. Автори визначають основні поняття, що лежать в основі безпеки хмар, та класифікують їх наступним чином: елементи віртуалізації, мульти-оренда, хмарна платформа та програмне забезпечення, аутсорсинг даних, безпека зберігання даних та стандартизація та довіра до провайдера. Також автори розглядають управління ризиками для кожної категорії. У дослідженні [9] проголошено, що поява хмарних вірусів пов'язана зі складною віртуалізованою інфраструктурою хмари та її динамічним характером, і вразливості можна поділити на три складові: По перше, багаторазовий доступ до хмари різних користувачів з усього світу несе відповідальність за виток інформації. По друге, користувачі хмар не знають розташування їх віртуальних машин, а провайдер не знає вміст віртуальних машин та програм, що дає шлях до загроз безпеки. По третє всі віртуалізовані сервери

підключені до обмеженої кількості мережевих карт, що призводить до більшої вразливості в віртуальному середовищі.

Підбиваючи підсумок, можна заявити, що на теперішній час немає єдиного наукового дослідження, що описує всі фактори ризику безпеки при впровадженні хмарних обчислень.

Формулювання цілей статті. Метою статті є розробка теоретико-методологічних підходів до визначення суті та особливостей оцінювання ризиків безпеки хмарних сервісів, виявлення основних компонентів ризику на кожному рівні хмари, та розробка схеми обчислення консолідованого індикатора безпеки для хмарних сервісів.

Основний матеріал дослідження. На нашу думку, жодна з розглянутих зарубіжними та вітчизняними дослідниками моделей оцінювання ризику безпеки цілком не є придатною для випадку міграції IT-інфраструктури підприємства до хмарного середовища, оскільки жодна з них не враховує особливостей внутрішньої взаємодії базових рівнів хмари, що є характерною ознакою хмарного середовища, та не враховує можливість віддаленого доступу до хмарних сервісів.

У зв'язку з цим викає потреба, оцінюючи хмарні ризики, визначати інформаційні ресурси, які потребують захисту. Ресурси можна розділити на дані, програми та процеси. Вплив на систему безпеки процесу міграції IT-інфраструктури до хмарного середовища залежить від моделі хмарних послуг та моделі розгортання хмари. Поєднання моделі обслуговування та моделі розгортання може допомогти визначити відповідний баланс безпеки для інформаційних ресурсів.

Ми можемо виділити наступні типи ризику, які впливають на хмарні ресурси:

- недоступність – хмарний ресурс недоступний, і він не може бути використаний споживачем.

- втрата – хмарний ресурс втрачається споживачем або його знищено.
- крадіжка – хмарних ресурс був навмисно вкрадений, і зараз він знаходиться в розпорядженні іншої фізичної особи / підприємства. Крадіжка є навмисною дією, яка може призвести до втрати даних.
- розкриття інформації – випадок, коли інформація стала доступною неавторизованому персоналу / підприємствам / організаціям або суспільству. Цей фактор також включає небажаний, але законний доступ до даних через міжнародні кордони.

Фактори ризику поділяються на критичні та регулярні. Зрозуміло, що збитки, що можуть бути завдані критичними факторами ризику безпеки, перевищують шкоду, яка може бути завдана регулярним ризикам даних. Критичні елементи хмарної інфраструктури, як правило, більш захищені, і тому ймовірність їх відмови нижче, ніж у звичайних елементів. Також варто звернути увагу, що фактор розкриття регулярних даних має низький ризик, тоді як фактор розкриття критичних даних має підвищений ризик. Крім того, тимчасова недоступність хмарних ресурсів може бути допустимою через низький рівень збитків. З іншого боку, крадіжка критичних даних зазвичай застрахована.

Для побудови консолідованої моделі пропонуємо використовувати вісім базових індикаторів для оцінювання ризиків (табл. 1).

Таблиця 1

Класифікація індикаторів оцінювання ризиків стану безпеки хмарного сервісу

Індикатор	Сутність індикатора
Захист трафіку даних	Забезпечення захисту трафіку даних
Зберігання даних	Рівень системи захисту хмарних сховищ даних
Аутентифікація користувачів	Рівень системи реєстрації користувачів та моніторинг часу їх роботи
Міра відокремлення користувачів	Розгортання додатків і баз даних кожного користувача в окремих віртуальних контейнерах

Відповідність вітчизняному законодавству	Міра додержання провайдером вітчизняного законодавства у сфері хмарних обчислень
Характеристика хмарного провайдера	Час реагування хмарного провайдера на події, міра залучення клієнтів до виправлення інцидентів
Система безпеки віртуальних машин	Забезпечення захисту віртуальних машин
Фізична безпека	Рівень забезпечення фізичного захисту хмарного провайдера
Система резервного копіювання даних	Забезпечення можливості відкату системи назад у разі пошкодження даних

Індикатори ризику мають бути розділені, відповідно до трьох шарів хмари, кожен ризик включає в себе показник збільшення ризику (Zb) або зменшення ризику (Zm). Крім того, необхідно врахувати їх вагу на загальну оцінку. Вага ризику зростає від недоступності до втрати, від втрати до крадіжки, від крадіжки до розкриття інформації.

Запропонована модель навмисно використовує узагальнюючий підхід для аналізу ефектів кожної комбінації: факторів ризику, типів ризику стану безпеки та хмарного провайдера. Для кожного з трьох шарів хмари (IaaS / PaaS / SaaS) обчислюються дві агреговані оцінки ризику: збільшення ризику (Zb) та зменшення ризику (Zm). Оцінка Zb пов'язана з факторною групою, яка частково орієнтована на коефіцієнти експозиції, тоді як Zm більше пов'язана з факторами захисту.

Таблиця 2 не тільки розрізняє коефіцієнти Zb / Zm, а також відображає ймовірність виникнення та прогнозовані збитки за кожним індикатором для чотирьох типів ризику (недоступність, втрата, крадіжка та розкриття). Вага кожного типу ризику є показником як ймовірності виникнення, так і очікуваного збитку від реалізації фактора ризику. У прикладі ймовірність та збитки класифікуються за 5-бальною шкалою (від 1 до 5), а ризиком є множення рейтингу ймовірності та збитку. Для кожного індикатора (фактору) кожен тип ризику оцінюється шляхом такого множення, що дає шкалу від 1 до 25. Таким чином, рівень ризику кожного індикатора ризику обчислюється шляхом підсумовування відповідних значень ризику за

чотирма типами ризику (недоступність, втрата, викрадення, та розкриття інформації). Приклад розрахунку коефіцієнтів ваги для індикаторів збільшення ризику стану безпеки для моделі IaaS наведено в таблиці 2.

Таблиця 2

Приклад розрахунку коефіцієнтів ваги для індикаторів ризику стану безпекі для моделі IaaS (фактори збільшення ризику)

IAAS: Індикатори ризику стану безпеки для моделі IaaS	**Недоступність** (I–ймовірність, Z– збитки, V–рівень ризику)			**Втрата** (I–ймовірність, Z– збитки, V–рівень ризику)			**Крадіжка** (I–ймовірність, Z– збитки, V–рівень ризику)			**Розкриття інформації** (I–ймовірність, Z–збитки, V–рівень ризику)		
Показники збільшення ризику (Zb)	I (1-5)	Z (1)	V (V=I*Z)	I (1-5)	Z (2)	V (V=I*Z)	I (1-5)	Z (3)	V (V=I*Z)	I (1-5)	Z (4)	V (V=I*Z)
1.Відповідність вітчизняному законодавству										2	4	2*4=8
2.Міра відокремлення користувачів (multitenance)							1	3	1*3=3	1	4	1*4=4
3.Аутентифікація користувачів	3	1	3*1=3	3	2	3*2=6	3	3	3*3=9	3	4	3*4=12
4.Система резервного копіювання даних	3	1	3*1=3	4	2	4*2=8						
5.Фізична безпека							3	3	3*3=9	3	4	3*4=12
6.Зберігання даних										3	4	3*4=12
7.Захист трафіка даних	2	1	2*1=2	2	2	2*2=4	2	3	2*3=6	4	4	4*4=16
8.Система безпеки віртуальних машин	3	1	3*1=3	2	2	2*2=4	2	3	2*3=6	3	4	3*4=12
9.Характеристика хмарного провайдера	2	1	2*1=2	3	2	3*2=6	3	3	3*3=9	3	4	3*4=12

Приклад розрахунку коефіцієнтів ваги для індикаторів зменшення ризику стану безпекі для моделі IaaS наведено в таблиці 3.

Таблиця 3

Приклад розрахунку коефіцієнтів ваги для індикаторів ризику стану безпеки для моделі IaaS (фактори зменшення ризику)

IAAS: Індикатори ризику стану безпеки Показники зменшення ризику (Zm)	**Недоступність** (I–ймовірність, Z– збитки, V–рівень ризику)			**Втрата** (I–ймовірність, Z– збитки, V–рівень ризику)			**Крадіжка** (I–ймовірність, Z– збитки, V–рівень ризику)			**Розкриття інформації** (I–ймовірність, Z– збитки, V–рівень ризику)		
	I (1-5)	Z (1)	V (V=I*Z)	I (1-5)	Z (2)	V (V=I*Z)	I (1-5)	Z (3)	V (V=I*Z)	I (1-5)	Z (4)	V (V=I*Z)
1.Масштабованість та еластичність хмарних обчислень	2	1	2*1=2									
2.Система аварійного відновлення та резервного копіювання	4	1	4*1=4	4	2	4*2=8	3	3	3*3=9			
3.Система оновлення ПЗ	2	1	2*1=2	3	2	3*2=6	4	3	4*3=12	2	4	2*4=8

Аналогічно проводиться розрахунок для моделей PaaS та SaaS. Проводиться агрегація ризиків кожного фактору ризику та їм надається вага, пропорційна їх внеску в загальне оцінювання ризику цієї категорії (категорія визначається моделлю надання послуг IaaS/PaaS/SaaS та одним з показників Zb / Zm). Коли всі ризики всіх рівнів хмари категорій (Zb або Zm) відомі, вони підсумовуються і кожний коефіцієнт ризику (% ваги) обчислюється як частка, яка сприяє загальному індикатору рівню ризику.

Цей приклад показує, що організації повинні стежити за процесом прийняття рішень відносно міграції до хмарного середовища, щоб знайти найкраще рішення кожного разу, коли новий хмарний провайдер виходить на ринок, покращуючи тим самим свої оцінки ризиків безпеки. Крім того, динамічна модель дозволяє досягти підвищеної оцінки ризиків відносно використання традиційних моделей.

Розрахунок складових консолідованого індикатора стану безпеки хмарного сервісу здійснюється таким способом: вони порівнюються зі стандартами виходячи з наданої інформації від провайдера хмарного сервісу; фахівці визначають рівень їх відповідності стандартам безпеки хмарних сервісів, використовуючи теорію нечітких множин, та розраховують уже консолідовані значення індикаторів.

Розрахунок зведеного індикатора безпеки хмарного сервісу провадиться за формулою

$$P_{ib} = k_1 * Z_{bd} + k_2 * Z_t + k_3 * \text{Aut} + k_4 * I_k + k_5 * N_p + k_6 * ZR_c + k_7 * Z_{vm} + k_8 * CR, \quad (1)$$

де P_{ib} – зведений індикатор безпеки хмарного сервісу;

Z_t — індикатор стану системи захисту трафіка даних хмари;

Z_{bd} — відносний індикатор захисту сховищ даних (експертна оцінка);

Aut — індикатор роботи системи реєстрації користувачів;

I_k — відносний індикатор віртуалізації контейнерів з даними користувачів;

N_p — індикатор стану відповідності вітчизняному законодавству;

R_c — індикатор роботи служби безпеки хмарного провайдера;

Z_{vm} — відносний індикатор стану системи захисту віртуальних машин (експертна оцінка);

CR — відносний індикатор якості системи резервного копіювання (експертна оцінка);

k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8 — коефіцієнти рівня впливу індикаторів на загальну оцінку.

Для уточнення розрахунків усі індикатори дістануть рівні (тобто коефіцієнти впливу на загальну оцінку). Визначають рівні впливу індикаторів фахівці за допомогою призначення ваг, беручи до уваги в аналізі

середньостатистичні бали показників та діапазон можливих значень індикатора.

Для ефективної конкуренції потрібні дві передумови, і запропоновані моделі оцінки ризику будуть ефективними. Автор вважає, що ринкові сили обов'язково змушують ці умови реалізуватися в довгостроковій перспективі. По-перше, хмарні постачальники повинні запропонувати стандартні функції своїх послуг, оскільки порівняння ймовірностей / збитків ризику має стосуватися подібних функцій. Це буде основою для порівняння розмірних оцінок ризику, пов'язаних із подібними послугами. По-друге, постачальники хмарних послугповинні будувати свої сервіси відповідно до відкритих стандартів (на сьогодні це не так), таким чином, забезпечуючи взаємозв'язок між різними сервісами хмарних провайдерів.

Висновки з даного дослідження і перспективи подальших досліджень у даному напрямі. Отже, запропонована модель дає можливість аналізувати ризики, що виникають під час упровадження конкретного хмарного сервісу, і на основі одержаних даних визначати важливість його створення або оренди для підприємства. Розроблена нами модель оцінювання дозволить провести максимальну систематизацію й автоматизувати всі етапи процесу оцінювання ризику під час розробки проекту хмарного сервісу та вибору його компонентів.

Подальші дослідження мають включати вдосконалення запропонованої методики для розрахунку оптимізованих рішень шляхом визначення пропорції між факторами збільшення / зменшення ризику, з метою визначення мінімального ризику. Також необхідно дослідити фактори ризику, які виникають при застосування різних моделей розгортання хмар та включити ці фактори ризику до запропонованої моделі.

Розглянуті методи та моделі можуть використовуватися в різних областях економіки та управління для оцінювання ризиків безпеки в проектах міграції IT-інфраструктур організацій до хмарних середовищ.

Література

1. P. Mell, and T. Grance, ―The NIST definition of cloud computing‖, National Institute of Standards and Technology, NIST, Vol. 53 No. 6, p. 50, 2009.
2. Weinhardt C., Anandasivam A., Blau B., Borissov N., Meini T., Michalk W. and Stosser J., "Cloud Computing – A Classification" / Business Models, and Research Directions, Bus. Models and Inform. Syst. Eng., vol. 1, no. 5, (2009) [Електроний ресурс]. – Режим доступу: http://aisel.aisnet.org/bise/vol1/iss5/6/
3. A. Gill, D. Banker, and P. Seltsika, "Moving Forward: Emerging Themes in Financial Services Technologies Adoption", Communications of the Association for Information Systems: Vol. 36, Article 12, 2015 [Електроний ресурс]. – Режим доступу: https://www.semanticscholar.org/paper/Moving-Forward%3A-Emerging-Themes-in-Financial-Gill-Bunker/99b1e6c3770de1067ace1d575e0727a87b8d58da
4. J. Bohli, N. Gruschka, M. Jensen, L.L. Iacono, and N. Marnau, "Security and Privacy-Enhancing Multi cloud Architectures", IEEE Transactions on Dependable and Secure Computing, Vol. 10, No' 4, 2013 [Електроний ресурс]. – Режим доступу:https://www.semanticscholar.org/paper/Security-and-Privacy-Enhancing-Multicloud-Bohli-Gruschka/0e8418f57749f77718f05f3db39b32353e8d1931
5. T. Ackermann, T. Widjaja, A. Benlian, and P. Buzmann, "Percieved IT Security Risks of Cloud Computing: Conceptualization and Scale Development, Thirty Third International Conference on Information Systems, Orlando USA, 2012. [Електроний ресурс]. – Режим доступу: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.665.7295&rep=rep1&type=pdf
6. C. A. Christiansen, C. J. Kolodgy, S. Hudson, and G. Pintal, IDC – White paper – "Identity and Access Management for Approaching Clouds", May

2010 [Електроний ресурс]. – Режим доступу: https://ru.scribd.com/document/82546531/Cloud-Security-Wp-236234-PDF

7. S. B. Yadav, and D. Tianxi, "A Comprehensive Method to Assess Work System Security Risk," Communications of the Association for Information Systems: Vol. 34, Article 8, 2014 [Електроний ресурс]. – Режим доступу: https://pdfs.semanticscholar.org/006e/d7e854fdb5d919b32fd74825bbb0180604ae.pdf
8. D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M Freire and P. R. M. Inácio, "Security issues in cloud environments: a survey", Int. J. Inf. Secur. 13:113–170, 2014 [Електроний ресурс]. – Режим доступу: http://www.di.ubi.pt/~mario/artigos/2013-IJIS.pdf
9. B. Mansukhani and T. A. Zia, "The Security Challemges and Countermeasures of Virtual Cloud", Australian Information Security Management Confference, 2012 [Електроний ресурс]. – Режим доступу: https://researchoutput.csu.edu.au/en/publications/the-security-challenges-and-countermeasures-of-virtual-cloud

References

1. P. Mell, and T. Grance, ―The NIST definition of cloud computing‖, National Institute of Standards and Technology, NIST, Vol. 53 No. 6, p. 50, 2009.
2. Weinhardt C., Anandasivam A., Blau B., Borissov N., Meini T., Michalk W. and Stosser J., "Cloud Computing – A Classification" //Business Models, and Research Directions, Bus. Models and Inform. Syst. Eng., vol. 1, no. 5, (2009) [Elektronyi resurs]. – Rezhym dostupu: http://aisel.aisnet.org/bise/vol1/iss5/6/
3. A. Gill, D. Banker, and P. Seltsika, "Moving Forward: Emerging Themes in Financial Services Technologies Adoption", Communications of the Association for Information Systems: Vol. 36, Article 12, 2015 [Elektronyi resurs]. – Rezhym dostupu: https://www.semanticscholar.org/paper/Moving-

Forward%3A-Emerging-Themes-in-Financial-Gill-Bunker/99b1e6c3770de1067ace1d575e0727a87b8d58da

4. J. Bohli, N. Gruschka, M. Jensen, L.L. Iacono, and N. Marnau, "Security and Privacy-Enhancing Multi cloud Architectures", IEEE Transactions on Dependable and Secure Computing, Vol. 10, No' 4, 2013 [Elektronyi resurs]. – Rezhym dostupu: https://www.semanticscholar.org/paper/Security-and-Privacy-Enhancing-Multicloud-Bohli-Gruschka/0e8418f57749f77718f05f3db39b32353e8d1931
5. T. Ackermann, T. Widjaja, A. Benlian, and P. Buzmann, "Percieved IT Security Risks of Cloud Computing: Conceptualization and Scale Development, Thirty Third International Conference on Information Systems, Orlando USA, 2012 [Elektronyi resurs]. – Rezhym dostupu: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.665.7295&rep=rep1&type=pdf
6. C. A. Christiansen, C. J. Kolodgy, S. Hudson, and G. Pintal, IDC – White paper – "Identity and Access Management for Approaching Clouds", May 2010 [Elektronyi resurs]. – Rezhym dostupu: https://ru.scribd.com/document/82546531/Cloud-Security-Wp-236234-PDF
7. S. B. Yadav, and D. Tianxi, "A Comprehensive Method to Assess Work System Security Risk," Communications of the Association for Information Systems: Vol. 34, Article 8, 2014 [Elektronyi resurs]. – Rezhym dostupu: https://pdfs.semanticscholar.org/006e/d7e854fdb5d919b32fd74825bbb0180604ae.pdf
8. D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M Freire and P. R. M. Inácio, "Security issues in cloud environments: a survey", Int. J. Inf. Secur. 13:113–170, 2014 [Elektronyi resurs]. – Rezhym dostupu: http://www.di.ubi.pt/~mario/artigos/2013-IJIS.pdf
9. B. Mansukhani and T. A. Zia, "The Security Challemges and Countermeasures of Virtual Cloud", Australian Information Security

Management Confference, 2012 [Elektronyi resurs]. – Rezhym dostupu: https://researchoutput.csu.edu.au/en/publications/the-security-challenges-and-countermeasures-of-virtual-cloud