На правах рукопису

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Одеська національна академія харчових технологій
Навчально-науковий інститут холоду,
кріотехнологій та екоенергетики
Факультет інформаційних технологій та кібербезпеки

XVI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

Матеріали конференції

Одеса
25–26 квітня 2016 р.

Стан, досягнення і перспективи інформаційних систем і технологій / Матеріали XVI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 25–26 квітня 2016 р. - Одеса, Видавництво ОНАХТ, 2016 р. - 176 с.

Збірник включає матеріали доповідей її учасників, які об'єднані по секціях кафедр: комп'ютерної інженерії (КІ), інформаційних технологій та кібербезпеки (ІТтаКБ).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова – д.т.н., проф., **Єгоров Б.В.,** ректор ОНАХТ.

Співголови :
Капрельянц Л.В. – д.т.н., проф., проректор з наукової роботи та міжнародних зв′язків,
Косой Б.В. – д.т.н., проф., в.о. директора ННІХКтаЕ ОНАХТ,
Котлик С.В. – к.т.н., доц., декан ФІТта КБ ОНАХТ,
Волков В.Е. – д.т.н., доц., директор ННІМАтаКС ОНАХТ,
Хобін В.А. – д.т.н., проф., завідувач кафедри автоматизації виробничих процесів ОНАХТ,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри технології і автоматизації виробництва радіоелектронних і електронно-обчислювальних засобів ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ "Львівська політехніка",
Тарасенко В. П. – д.т.н., проф., завідувач кафедри СПіСКС НТУУ «Київський політехнічний інститут»,
Жуков І. А. – д.т.н., проф., директор інституту комп'ютерних технологій Національного авіаційного університету.

<u>Члени оргкомітету:</u>
Плотніков В. М. – д.т.н., проф., завідувач кафедри інформаційних технологій та кібербезпеки ОНАХТ.
Артеменко С.В. – д.т.н., проф., в.о. завідувача кафедри комп'ютерної інженерії ОНАХТ.
Князєва Н.О. – д.т.н., проф. кафедри комп'ютерної інженерії ОНАХТ.
Грищенко І.В. – к.т.н., заступник декана ФІТта КБ ОНАХТ.
Шамрай О.А. – к.т.н., доц. кафедри ТДтаВЕ ОНАХТ.

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Шамрай О.А.

Список літератури:

1. http://app2top.ru/game_development/kak-napisat-horoshij-dizajn-dokument-44635.html - інтернет ресурс, стаття «Как написать хороший дизайн-документ?».
2. http://www.gamedis.ru/?p=113 – інтернет ресурс, стаття «Легкий способ написать дизайн документ».
3. https://ru.wikipedia.org/wiki /Дизайн-документ - інтернет ресурс, стаття «Дизайн документ».

ДОСЛІДЖЕННЯ ОСНОВНИХ МОДЕЛЕЙ ХМАРНИХ СЕРВІСІВ

Ільєв В.В. студент ОКР „бакалавр" факультету ІТ та КБ ОНАХТ
Керівник – ст. викл. каф. КІ Бондаренко В.Г.

В даний час широкого поширення набули розподілені інформаційні системи, що обумовлено розвитком обчислювальних мереж і зростанням виробництва обчислювальних пристроїв. При цьому існує необхідність обробки конфіденційної інформації, наприклад, персональних даних, що висуває підвищені вимоги до оцінки захищеності розподілених інформаційних систем. В даний час активно ведуться роботи, пов'язані з аналізом захищеності протоколів обміну даними. Актуальність цих робіт обумовлена, з одного боку необхідністю забезпечення інформаційні-ної безпеки в ході розподіленого інформаційного обміну, а з іншого - великий обчислювальною складністю дослідження захищеності інформаційних систем, побудованих на основі розроблених протоколів. Управління доступом дає гарантію, що тільки авторизовані користувачі мають доступ до даних і сервісів. Ця проблема стає складним завданням в розподілених системах, де координація діяльності центрального органу може виявитися неможливим або може бути вимоглива до ресурсів. Існують деякі сучасні проблеми доступу в розподілених системах, таких як мобільні мережі, транспортні мережі, інтелектуальні мережі та «хмарні обчислення». Кожне з цих додатків має різні обмеження і вимоги. Термін «хмарні обчислення» використовується досить широко, однак різні хмарні моделі мають відмінності один від одного з точки зору безпеки. Тому важливо, щоб організації не користувалися універсальним підходом для всіх моделей. Хмарні моделі можна розділити:

- програмне забезпечення як послуга (SoftwareasaService, SaaS);
- платформи як послуга (PlatformasaService, PaaS);
- інфраструктура як послуга (Integration as a Service, IaaS).

При забезпеченні безпеки хмари необхідно враховувати як відмінності між цими трьома видами хмарних моделей, так і їх загальні риси.

SaaS. Ця модель орієнтована на управління доступом до додатків. Наприклад, в політиках доступу може бути визначено, що агент з продажу має можливість завантажувати з програми для управління відносинами з клієнтами цілевказівки на замовників лише за певної місцевості або тільки в робочий час.

По суті, завдання директора з безпеки в разі SaaS - підготувати набір обмежень, які будуть регулювати доступ користувача до додатків.

PaaS. Дана модель орієнтована на захист даних, що особливо важливо в разі зберігання, що надається у вигляді сервісу. Для PaaS обов'язково слід враховувати ймовірність тимчасового виходу провайдера з ладу. З точки зору безпеки важливо забезпечити балансування навантаження між провайдерами, щоб перерозподілити її в разі відмови основного. Ще один ключовий момент - можливість шифрування даних при їх зберіганні на сторонньої платформі і знання нормативних актів, які можна застосувати до зберігання даних в різних країнах.

IaaS. При використанні такої моделі передбачається, що споживач формулює свій запит до хмари в термінах, необхідних йому обчислювальних ресурсів: кількість процесорів, оперативної пам'яті, дискового простору і мережних комунікацій. Самообслуговування в рамках такого сервісу передбачає можливість самостійного створення необхідної інфраструктури для бізнес-додатки у вигляді віртуальних машин, установки і налаштування прикладного ПО. При цьому хмара має механізм забезпечення доступності наданої інфраструктури і способи обліку споживання. Ця модель найбільш поширена на даний момент, так як добре вписується в найбільш часто використовувану структуру організації IT-департаментів.

Виходячи з вищевикладеного визначення хмарних обчислень, хмарні сервіси можна представити у вигляді багатошарової моделі, що складається з шарів: IaaS, PaaS, SaaS. Базисом або фундаментом хмарних сервісів є фізична інфраструктура (physicalinfrastructure), т. Е. Сервери, сховища, мережі та системне програмне забезпечення хмарного дата-центру (Clouddatacenter) або мережі взаємопов'язаних хмарних дата-центрів.

Перший шар хмарних послуг - IaaS (інфраструктура).

Другий шар - PaaS (програмна платформа).

Третій шар - SaaS (хмарне додаток).

Список літератури

1. Vladimir Ruchkin, Vitaliy Romanchuk and Roman Sulitsa. Clustering, Restorability and Designing Of Embedded Computer System Based On Neuroprocessors // Proceedings of the 2nd Mediterranean Conference on Embedded Computing (MECO). - Budva, Montenegro, 2013.- c.58–62.
2. Романчук В. А. Логическое проектирование вычислительных систем на базе нейропроцессоров // Современные научные исследования и инновации. 2014. № 12. [Электронний ресурс]. Режим доступу: http://web.snauka.ru/issues/ (дата звернення 20.03.16)..
3. Макаров Д. В., Романчук В. А. Облачные SaaS, IaaS, PaaS системы для искусственного интеллекта // Современная техника и технологии. 2015. № 5 [Электронний ресурс]. Режим доступу: http://technology.snauka.ru/2015/05/6731 (дата звернення 20.03.16).