

УДК 004.056.53+638.14.071+638.14.075

М.С. МЕДВЕДЧУК, О.А. ПАСІЧНИК, Т.К. СКРИПНИК

Хмельницький національний університет

ІНФОРМАЦІЙНА БЕЗПЕКА ХМАРНИХ СЕРВІСІВ У ПРОВАДЖЕННІ БДЖІЛЬНИЦЬКОГО ГОСПОДАРСТВА

В статті досліджено сучасний стан впровадження інформаційних технологій з використанням хмарних сервісів у бджільництві. Охарактеризовано технологію хмарних сервісів, визначено перспективи її розвитку та проаналізовано питання та принципи реалізації безпекових аспектів під час застосування в бджільництві. Цінність роботи полягає в тому, що проведені дослідження дозволили зрозуміти, що можливості хмарних технологій та сервісів дозволяють розв'язувати завдання бізнесу та надають реальні перспективи для ефективного впровадження інформаційних технологій у бджільництві.

Ключові слова: хмарні сервіси, інформаційна безпека, бджільництво, бази даних, захист персональних даних, нанотехнології, аналіз.

M.S. MEDVEDCHUK, O.A. PASICHNYK, T.K. SKRYPNYK

Khmelnytsky National University

INFORMATION SECURITY OF CLOUD SERVICES IN BEEKEEPING PROCEEDINGS

The current state of information technology with usage of cloud services in beekeeping has been investigated in this article. Cloud services technology has been characterized, perspectives of it's growth have been defined and questions and implementation principles of safety aspects while using it in beekeeping have been analyzed. The value of the work is that the explorations helped to understand that the possibility of cloud technologies and services allow to solve business problems and provide real prospects for effective implementation of information technology in beekeeping.

Keywords: cloud services, information security, beekeeping, databases, personal data protection, nanotechnology, analysis.

Постановка проблеми. Інтенсифікація інноваційних процесів, розвиток інформаційних технологій, їх проникнення в усі сфери життєво важливих інтересів зумовили підкорення сфери фермерського господарства, що крім безперечних переваг призводить до появи низки стратегічних проблем. Посилюється небезпека несанкціонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем. Проблеми захисту інформації потребують комплексного підходу, тобто створення системи інформаційної безпеки (ІБ).

Сучасні фермерські господарства знаходяться під постійним впливом факторів, пов'язаних з розвитком технологій, які, з одного боку, спрощують роботу з великими обсягами інформації, проте, з іншого – зумовлюють проблеми, пов'язані насамперед з інформаційною безпекою. Не виключенням відмітилось впровадження програмного забезпечення у бджільництві. На заміну стереотипним паперовим журналам-зміткам бджільника, які зазвичай загублювались або з часом просто набували не читабельного стану, було використано інформаційні технології.

Одним з сучасних та перспективних напрямків інформатизації є хмарні сервіси (хмарні обчислення), що з'явилися в 2006 році, коли Amazon's Elastic Computing Cloud побудували свої дата-центри. Багато підприємств, які займалися інформаційними технологіями, створювали підґрунтя для можливості реалізації збереження та обробки даних на віддалених, спеціально виділених серверах, що в подальшому отримало назву «хмарних технологій». Пізніше з'являються такі продукти, як Google's MapReduce, Microsoft's Windows Azure, iCloud, Amazon CloudDrive тощо. Особливо цікавим з комерційної точки зору є можливість безкоштовного використання, хоча й з певними обмеженнями, які здебільшого не стосуються кінцевої функціональності.

Суттєвою та характерною особливістю хмарних технологій є віддалений, технічно та територіально відокремлений механізм збереження даних, що піднімає на принципово новий щабель питання їх конфіденційності та обмеження несанкціонованого доступу.

Стан дослідження. Проблеми безпеки діяльності, фінансової та інформаційної безпеки є актуальними і набули широкого висвітлення у вітчизняній і зарубіжній науці. Питанням інформаційної безпеки присвячені дослідження таких вітчизняних науковців: Г.С. Гриджука [1], Б. А. Кормича [2], В. Л. Гевко, а також російських учених, таких як Е.Б. Белов, В. П. Лось, Р.В. Мещеряков, А.А. Шелупанов [3].

Слід зазначити, що дослідження теоретичних і практичних засад функціонування хмарних сервісів у вітчизняній науці ще не набули достатнього поширення як проблема загалом, так й зокрема для роботи фермерських господарств.

Метою статті є аналіз теоретичних і практичних аспектів інформаційної безпеки хмарних технологій для впровадження у сфері фермерського господарства бджільництва з визначення їх принципів і перспектив.

Виклад основних положень. Інформаційна безпека підприємства – це захист інформації, якою володіє підприємство від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок під час надходження. Крім того, під інформаційною безпекою розуміють захищеність інформації та підтримуючої її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може бути нанесення

шкоди самій інформації, її власникам або підтримуючій інфраструктурі [3].

Архітектура ІБ охоплює процеси, людей, технології, різні типи інформації, адаптуючись до них, враховує складність і мінливість сучасного підприємства. Іншими словами, вона описує бажану структуру інфраструктури безпеки організації й інших, пов'язаних з інформаційною безпекою, компонентів та інтерфейсів.

Поділяють мету системи безпеки на такі події: захист прав підприємства (установи), його структурних підрозділів і співробітників, збереження й ефективне використання інформаційних, матеріальних і фінансових ресурсів, підвищення іміджу системи за рахунок забезпечення якості послуг щодо інформаційної безпеки.

Поява хмарних технологій спровокувала розгортання великомасштабних розподілених систем постачальників програмного забезпечення для широкого кола кінцевих споживачів.

Хмарні системи забезпечують просту й уніфіковану взаємодію між постачальником і користувачем та включають програмне забезпечення, тобто сервісну підсистему введення, виведення інформації та базу даних для довготривалого їх зберігання з багаторазовим доступом. Ці системи динамічно розподіляють обчислювальні ресурси у відповідь на запити про резервування ресурсу користувачем з дотриманням певних стандартів якості обслуговування користувачів.

Хмарні технології загалом й обчислення зокрема (англ. cloud computing) – це технологія розподіленої обробки та збереження даних, в якій комп'ютерні ресурси та потужності надаються користувачам як Інтернет-сервіс [2]. Хмарний сервіс є особливою клієнт-серверною технологією, яка передбачає використання клієнтом ресурсів групи серверів у мережі, які взаємодіють так [2]:

- для клієнта вся група виглядає як єдиний віртуальний сервер;
- клієнт може прозоро та гнучко змінювати обсяги споживання ресурсів у разі зміни своїх потреб.

Під час використання хмарних технологій користувач має доступ до власних даних, але не може керувати та не повинен піклуватися про інфраструктуру, операційну систему і програмне забезпечення, з якими він працює. «Хмарою» називають Інтернет, який приховує усі технічні деталі.

Таблиця 1

Переваги та недоліки хмарних сервісів

Переваги	Недоліки
<ul style="list-style-type: none"> • Не потрібен сучасний потужний комп'ютер для виконання складної обробки інформації • Збільшення обчислювальних потужностей за потребою • Менші витрати на ПЗ; найсучасніші версії ПЗ • «Хмара» пропонує віртуально необмежений простір для зберігання інформації • Надійність збереження даних, комп'ютерний збій у «хмарі» не призведе до втрати даних • У «хмарі» не має значення, якою операційною системою користується користувач • Хмарні сервіси значно скорочують апаратне та програмне • Можливість багатьох користувачів легко організовувати спільну роботу над документами і проектами 	<ul style="list-style-type: none"> • Технологія є вимогливою щодо доступу до Інтернету, його безперебійності та швидкодії; бувають випадки, коли сервер може бути недоступний, і тоді ця послуга стає неможливою • Аспекти безпеки даних; Закон України «Про захист персональних даних» не передбачає використання хмарних сервісів • Малоефективна робота у разі низької швидкості каналу зв'язку • Велика кількість ризиків втрати інформаційних даних, серед яких найголовнішими є ризик захоплення даних на шляху від компанії до сервера

Хмарні системи дозволяють мати доступ до інформації та серверів з будь-якого місця світу, звільнивши користувачів від необхідності мати стаціонарний комп'ютер та зробивши доступнішою спільну роботу багатьох людей, які можуть знаходитися в різних місцях.

Аналіз хмарних технологій, як і будь-якої технології, що швидко розвивається, повинен враховувати як переваги, так і недоліки (табл. 1).

Вимоги до безпеки на основі аналізу HDFS HDFS (HadoopDistributed File System) є відомою поширеною технологією хмарних обчислень [4].

Аналізуючи HDFS, вимоги безпеки до хмарних обчислень можна поділити на такі групи [5]:

Перевірка достовірності Логіна клієнта: більшість хмарних обчислень перевіряють браузер клієнта і проводять ідентифікацію користувача згідно із запитом програм хмарних обчислень для первинної потреби.

• Присутність одиничної помилки з Вузлом імені: якщо Вузол імені атакують або зламують, це може призвести до катастрофічних наслідків у системі. Тому ефективність Вузла імені в хмарних обчисленнях і його дієвість – це ключ до успіху в інформаційній безпеці. Посилення захисту Вузла імені є критично важливим.

• Швидке відновлення блоків даних і контроль за правом читання/запису: Вузол даних (DataNode) – це вузол накопичення даних, де можливі проблеми та труднощі з доступом до даних.

Принципи захисту даних. Уся процедура захисту даних побудована на конфіденційності, цілісності

та доступності. Конфіденційність належить до так званої прихованої функції фактичних даних або інформації і є однією із найжорсткіших вимог інформаційної безпеки. У випадку хмарних обчислень дані накопичуються в центрах обробки даних, де безпека та конфіденційність даних ще важливіші. Цілісність даних у будь-якому вигляді не відіграє значної ролі для гарантії несанкціонованого видалення, зміни або пошкодження. Доступність даних означає, що користувачі можуть використовувати дані за рахунок використання потенціальних можливостей хмарних технологій.

Модель захисту даних. У моделі використовується тришарова захисна структура системи [4].

- Перший шар відповідає за автентифікацію користувачів цифрових сертифікатів, виданих відповідними органами.

- Другий шар відповідальний за шифрування даних користувача.

- Третій шар – використання даних користувача для швидкого відновлення.

За допомогою трирівневої структури автентифікація користувача використовується для забезпечення цілісності даних. Через функцію захисту конфіденційності небезпечний користувач не зможе отримати повного доступу до інформації, що дуже важливо для захисту комерційних таємниць ділових користувачів у середовищі хмарних обчислень.

Таблиця 2

Основні принципи безпеки для хмарних обчислень

№ з/п	Принципи	Коротка характеристика принципів
1.	Прозорість	Компанії-провайдери розкривають внутрішні правила обробки інформації, а також відомості про діяльність
2.	Обмеження за сферами використання	Компанії не претендують на володіння даними замовників і можуть використовувати їх лише в тих цілях, для яких вони були отримані від замовників
3.	Розкриття	Компанії розкривають дані замовників лише у випадку, якщо це потрібно самим замовникам або передбачено законом, і повинні в такому разі повідомляти замовників про розкриття даних на вимогу правоохоронних органів у тій частині, наскільки це дозволяє законодавство
4.	Система управління безпекою	Компанії володіють потужною системою захисту даних, що відповідає міжнародним стандартам (таким, як ISO 27002)
5.	Додаткові можливості у сфері безпеки	Компанії зобов'язуються пропонувати замовникам додаткові можливості щодо захисту їх даних
6.	Розміщення даних	Компанії надають замовникам список країн, в яких розміщуються пов'язані з ними дані
7.	Повідомлення про витоки інформації	Компанії оперативно повідомляють замовників про всі відомі витоки, які ставлять під загрозу конфіденційність або цілісність даних
8.	Аудит	Компанії звертаються до послуг сторонніх аудиторів з метою перевірки того, наскільки їх система управління безпекою відповідає вимогам відповідних стандартів

Інтернет став платформою для розподілених додатків: компанія може вести конфіденційний внутрішній документообіг на чужих потужностях, уклавши контракт зі стороннім SaaS-постачальником, який, в свою чергу, буде обробляти отримані дані на обчислювальних потужностях інших постачальників послуг IaaS і PaaS.

NIST запропонував набір із п'яти базових принципів безпеки для хмарних обчислень (див. табл. 2) [5].

Незважаючи на те, що зазначені пропозиції не набули широкої підтримки учасників галузі, найімовірніше, в майбутньому дискусія призведе до вироблення загальногалузових правил – спочатку в США і Європі, а пізніше, можливо й одночасно, в інших країнах. Це сприятиме регулюванню інтересів користувачів і постачальників хмарних послуг.

Українське законодавство поки що не надає хмарним технологіям особливої уваги. Насамперед немає розробленого договору двох сторін, який би врегульовував відносини між користувачем та провайдером, що надає хмарні потужності, водночас як у Європі процес оновлення законодавства в цьому напрямі досить активний.

Питання інформаційної безпеки є особливо актуальним для сфери бджільництва, яке є дрібним або, максимум, середнім бізнесом й, внаслідок цього, відзначається низькою стресостійкістю в питаннях втрати даних.

Висновки. Ідея доступних комп'ютерних послуг стає реальністю. Можливості «хмар» дозволяють розв'язувати завдання бізнесу та надають реальні перспективи для інформаційних технологій у бджільництві. Центри обробки даних отримують можливість надавати свої послуги більшій кількості користувачів. Пасічники можуть думати про нові генерації своїх продуктів.

Передбачають, що масової міграції комерційних структур у публічні «хмари» не буде, повної

відмови від власних ручних записів також не передбачається, але пасічники прийдуть до гібридної моделі, де збережуться обидва елементи.

Програмні застосування майбутнього матимуть частину, що працює на комп'ютері користувача, та частину, що працює у «хмарі», причому хмарна частка повинна швидко розширюватись для роботи з тисячами серверів у разі потреби, а також зменшуватись на одній віртуальній машині.

Питання інформаційної безпеки технології хмарних сервісів, особливо в ході використання в бджільництві, потребують підвищеної уваги, а в багатьох аспектах – першочергових розробок і напрацювань.

Література

1. Гридчук Г. С. Систематизація методів інформаційної безпеки [Електронний ресурс] / Г. С. Гридчук. – Режим доступу : <http://www.nbu.gov.ua/portal/natural/Vntu/2009/pdf/64.pdf>
2. Кормич Б. А. Інформаційна безпека: організаційно-правові основи : навч. посібник / Б. А. Кормич. – К. : Кондор, 2004. – 384 с.
3. Белов Е. Б. Основы информационной безопасности: учеб. пособие / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М. : Горячая линия-Телеком, 2006. – 544 с.
4. Гудзовата О. О. Інформаційна безпека хмарних сервісів / О. О. Гудзовата // Львівський державний університет внутрішніх справ журнал. – 2013. – № 2. – С. 228–239.
5. Гудзовата О. О. Хмарні сервіси: можливості, безпека, перспективи : колективна монографія : у 4 т. / О. О. Гудзовата // Теоретичні та прикладні аспекти підвищення конкурентоспроможності підприємств. – Дніпропетровськ : «Герда», 2013. – Т. 1. – С. 102–110.
6. Бондар Є. С. Хмарні обчислення та їх застосування / Є. С. Бондар, М. М. Глибовець, С. С. Гороховський // Вісник КНУ ім. Т. Шевченка. – К. : КНУ, 2011. – Вип. № 1. – С. 74–82.

Рецензія/Peer review : 7.1.2017 р. Надрукована/Printed : 5.2.2017 р.

Рецензент : д.т.н., проф. Сорокати Р.В.