УДК 004:378.091.31
DOI https://doi.org/10.32782/2663-5941/2025.1.2/30

Прозур В.О.
Навчально-науковий інститут «Український державний хіміко-технологічний університет»
Українського державного університету науки і технологій

ВТРУЧАННЯ У ХМАРНІ СЕРВІСИ: НОВІ ВИКЛИКИ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Метою цієї статті є дослідження хмарних сервісів та їхніх можливостей та викликів. Стаття присвячена дослідженню питань побудови та ефективності використання хмарних сервісів для побудови інформаційної безпеки. Визначено основні засади функціонування автоматизованих систем керування хмарними сервісами. Особливостями запропонованої архітектури є використання портальних технологій, автоматичного управління ресурсами та гібридної хмарної інфраструктури. Різноманітні дослідницькі проблеми визначаються з точки зору зберігання розподілених баз даних, безпеки даних, неоднорідності та візуалізація даних у хмарних сервісах. З останнім прогресом комп'ютерних технологій кількість доступних хмарних сервісів збільшується день за днем. Однак надмірні обсяги даних створюють великі проблеми для користувачів. Тим часом, хмарні сервіси забезпечують потужне середовище для зберігання великих обсягів даних. Результати дослідження: описують підходи до захисту хмарних сервісів залежно від категорії інфраструктури, що використовується – приватні/публічні. Проведено порівняльний аналіз поділу відповідальності між провайдером та користувачем таких хмарних сервісів, як IaaS, PaaS, SaaS. Аналіз показав, що компанії забезпечують захист усіх рівнів хмарної інфраструктури самостійно у разі використання приватного хмарного сервісу. В разі використання публічного хмарного сервісу – за компанією залишається менший контроль за захистом, що дозволяє заощадити кошти на обслуговуючих фахівців, але позбавляє можливості вносити суттєві зміни до поточної інфраструктури для відповідності вимогам регуляторів. Практична значущість дослідження підтверджується визначенням набору практичних рекомендацій щодо усунення основних загроз хмарної інфраструктури шляхом застосування засобів захисту різних класів, приклади яких представлені у роботі.

Ключові слова: *хмарні обчислення, засоби захисту, бази даних, гібридні хмарні інфраструктури, публічний хмарний сервіс.*

Постановка проблеми. Актуальність використання на сьогоднішній день хмарних ресурсів очевидна, зростання їх можливостей у різних сферах стає все більш значним, а самі хмарні технології вже виділяються в окрему галузь ринку інформаційних технологій. При цьому цілком очевидно, що поряд зі стрімким зростанням використання хмарних систем та їх яскраво вираженими перевагами зростає також кількість нових ризиків та загроз, технологічного та правового характеру, які обов'язково мають бути досліджені.

Зародження хмарних технологій відбулося 1963 року за ініціативи Міністерства оборони США. В основі досліджень лежало створення принципово нової системи розподілу часу для поява можливості організації спільного доступу до ресурсів електронно-обчислювальних машин (ЕОМ) паралельно кільком віддаленим користувачам. В основу цих досліджень лягла експериментальна система Compatible Time-Sharing System (CTSS), вчені отримали можливість підключатися до одного. Використовуючи попередні напрацювання, до 1971 року було створено найбільш сучасна розрахована на багато користувачів операційна система UNIX [1].

Наступними важливими кроками у розвитку хмарних технологій стали можливість підключення до глобальної мережі та поява віртуальних машин. З розвитком інтернету широке поширення отримали онлайн-сервіси – SaaS (Software as a Service – програмне забезпечення як послуга), в яких користувачу надавалася можливість працювати з програмним забезпеченням віддалено через мережу Інтернет (рис. 1) [2].

В даний час обсяг хмарних послуг в Україні інтенсивно зростає, проявляється тенденція співробітництва міжнародних компаній із провайдерами хмарних сервісів. Це підтверджує міжнародна дослідна компанія IDC (International Data Corporation) у своїй роботі «Ринок хмарних послуг України перевищив мільярд доларів», а також статистика найбільших інтеграторів у сфері інформаційних технологій, це пов'язано з збільшенням проектів, пов'язаних із хмарним середовищем.

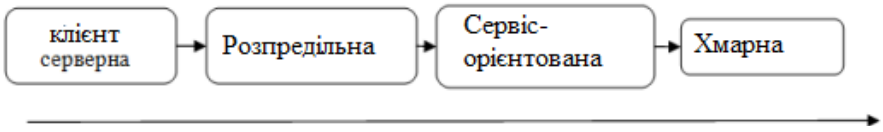

Рис. 1. Послідовність розвитку концепцій [2]

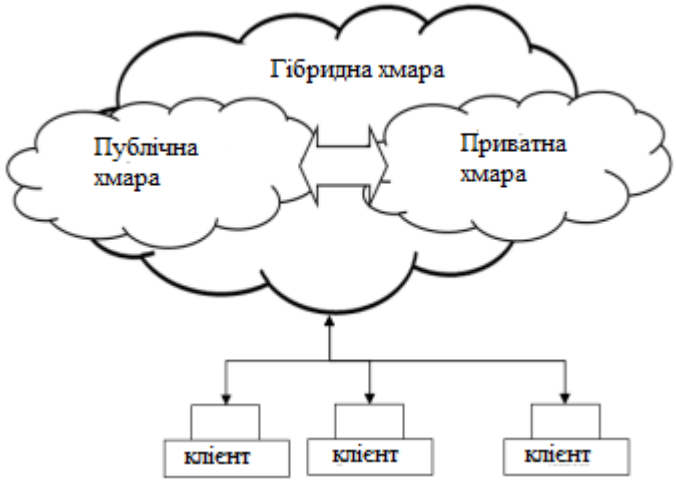

Рис. 2. Гібридна хмарна інфраструктура [7]

Історія з пандемією COVID-19 наголошує, що бізнес-процеси у найбільших підприємствах вимагають такого рівня інформатизації, щоб у працівників був доступ до ресурсів бізнес-процесів у будь-який час і з будь-якої точки світу. А використання хмарних технологій дозволить забезпечувати необхідний рівень доступності [3]. Все це говорить про те, що питання безпеки хмарних серверів як ніколи актуальні. Водночас особливої гостроти набуває проблематика щодо забезпечення безпеки, включаючи захист інформації під час використання хмарних технологій.

Аналіз останніх досліджень і публікацій. Сьогодні хмарні системи класифікують за моделями розгортання, визначальним розміщення та доступ до даних, і за моделями обслуговування, визначальним тип та обсяги наданих послуг [4]. За моделлю розгортання автори [5] розрізняють такі види:

– Приватна хмара – це інфраструктура, обмежена групою користувачів, найчастіше у межах співробітників однієї компанії. У цьому випадку ніхто крім них (т.к. доступ може бути обмежений на фізичному рівні) не може отримати доступ до даних, тим самим забезпечуючи безпеку даних.

– Публічна хмара – це інфраструктура для вільного використання широким спектром користувачів. Дозвіл доступу великої кількості різних користувачів ставить під великі ризики витоку та втрати даних.

– Громадська хмара – вид інфраструктури для групи або кількох груп мають спільні завдання та цілі.

Як зазначає Khan із співавторами [6] публічна хмара надає зручний та вільний доступ до даних, але через це є вразливим. Приватна хмара, у свою чергу, надає доступ до даних обмеженій кількості користувачів, наприклад, усередині однієї компанії, цим забезпечуючи ізольованість даних, отже їх безпеку. Надати зручний доступ та убезпечити дані дозволяє об'єднання даних моделей у гібридну хмару. Гібридна хмара – це комбінація, що поєднує дві і більше різних хмарних інфраструктур. Поділ хмари на публічну та приватну частини, дозволяє забезпечити безпеку даних у приватній частині та вільний доступ до даних у публічній частині, як показано на рис. 2 [7].

Le Duc з колегами [8] виділяють три види хмарних сервісів: інфраструктура як послуга (IaaS), платформа як послуга (PaaS) та програмне забезпечення як послуга (SaaS). У зв'язку з цим слід зазначити зроблену наприкінці 2022 року заяву компанії «Trend Micro», одного з лідерів серед постачальників комплексних засобів захисту «хмар», про те, що наявні наразі засоби безпеки поки що не здатні повною мірою забезпечити захист даних у хмарних серверах [9]. Як зазначається в [10] ця проблема є актуальною, адже однією з ключових компаній на міжнародному ринку програмного забезпечення в галузі інформаційної безпеки та

антивірусів корпорацією «Symantec», зроблено висновок у тому, що 77% підприємств відчувають труднощі через самовільне використання персоналом хмарних ресурсів в обхід правил підприємства, що призводить до порушень цілісності чи втрати конфіденційної інформації. Саме з цієї причини на особливу увагу заслуговують аспекти правового регулювання використання хмарних технологій і витікаючих з цього ризиків.

У класичній моделі забезпечення інформаційної безпеки контроль якості здійснюється перед використанням системи [11]. У сучасній моделі необхідно постійно контролювати рівень виконання вимог безпеки: аналізувати якість та моніторити здоров'я хмарної системи. Alsolami E. [12] наголошує, що забезпечення інформаційної безпеки у хмарі – комплексне завдання, яка досягається за рахунок комбінації «технології – процеси» і включає наступні основні компоненти:

a) класичні підходи (контроль доступу до хмари, захист від шкідливого програмного забезпечення, захист периметра та ін.);

b) процеси (процеси забезпечення інформаційної безпеки для класичної інфраструктури: управління доступом, управління інцидентами, управління вразливістю інфраструктури, управління ризиками – все це необхідно адаптувати до специфіки хмари, її інструментарію та моделі поділу відповідальності; унікальних процесів для сучасної інфраструктури);

c) хмарні підходи (індивідуальні підходи для унікальних хмар (використання вбудованих інструментів забезпечення інформаційної безпеки хмари, шифрування даних у хмарі, вибір хмарного провайдера з урахуванням можливостей інформаційної безпеки та ін.).

Проблема погіршується ще й тим, що, розміщуючи інформацію в публічному хмарному сервісі, організація не має можливості контролювати рівень забезпечення її безпеки через те, що провайдери хмарних сервісів не надають клієнтам можливість проведення статистичного контролю захищеності своїх сервісів.

Постановка завдання. Метою статті є дослідження хмарних баз даних, їхніх можливостей та викликів у впровадженні в освітній, науковий та технічний процес.

Виклад основного матеріалу. Серед найбільш актуальних загроз як у приватній, так і публічній сервісній хмарі, виділяються наступні:

• недостатній рівень інформаційної безпеки (ІБ) провайдера;

• неконтрольований доступ до хмарних сервісів [13];

• перехоплення контролю над ресурсами у хмарі;

• несанкціонований доступ до Application programming interface (API);

• витік конфіденційних даних із хмари;

• використання «тіньових ІТ».

У разі приватних та публічних хмар з'являється питання поділу відповідальності (табл. 1) між провайдером та користувачем хмарних сервісів. Ця таблиця – концептуальна, залежно від хмарного провайдера та конкретного сервісу, який буде використовуватися у сервісній хмарі, сам поділ відповідальності може змінюватися. У випадках приватної хмари компанія забезпечує захист на всіх рівнях від фізичної інфраструктури до рівня тих даних, що обробляються у хмарній платформі. У разі публічної хмари провайдер та користувач беруть на себе частину відповідальності, організуючи спільну роботу. Таким чином, за клієнтом залишається менший контроль, ніж у власній інфраструктурі. Це допомагає заощадити, але підвищує важливість контролю, що залишається на стороні клієнта [15].

Таблиця 1

Розподіл обов'язків між провайдером та користувачем [15]

Об'єкти	**Приватні хмари**	**Громадські сервісні хмари**			**Особливості**
	IaaS/PaaS/SaaS	IaaS	PaaS	SaaS	
Дані	–	–	–	–	Підвищення важливості ІБ високих рівнів (немає можливості компенсувати низькорівневими «контролями»)
Кінцеві пристрої та користувачі	–		–	–	
Управління доступом	–	–		–	
Програми	–	–		+	Передача провайдеру витрат на підтримку контролю; збільшення важливості контрактів та угод про рівень сервісу
Мережа	–			+	
Хости	–			+	
Фізична безпека	–			+	
Позначення:		– відповідальність користувача + відповідальність провайдера сервісних хмарних послуг			

Особливість захисту хмарного сервісу випливає із високого ступеня автоматизації хмарних платформ: підвищується динамічність того ландшафту, що у хмарі може бути розгорнутий. Якщо раніше можна було обійтися ручними «контролем» (ручним адмініструванням та реалізацією вимог ІБ), то на даний час у сервісній хмарі такий контроль не встигає за темпами хмари. Для своєчасного виявлення та контролю всіх змін в інфраструктурі сервісної хмари необхідно впроваджувати автоматизацію контролю ІБ та використовувати вже готові шаблони.

Раніше основа безпеки хмарних середовищ полягала у захисті мережевого периметра від зовнішніх загроз. У зв'язку із нинішньою віддаленою роботою через пандемію та військові дії грань мережевого периметра розмивається. Співробітники компаній, які використовують хмарні послуги, виходять за межі мережного периметра при підключенні до внутрішніх систем через незахищені канали зв'язку, а також «споживають» хмарні програми, які мають на увазі передачу будь-яких даних та процесів поза контрольованим мережевим периметром. Отже, у сучасній інфраструктурі захист тільки мережевого периметра недостатній, що веде до необхідності забезпечення захисту на всіх рівнях: мережа, програми, доступ, дані.

Розширене бачення захистів хмар ґрунтується на кращих міжнародних практиках, вироблених за більш ніж 10 років існування хмар, а також на практиці побудови хмарних платформ та міграції інфраструктури з традиційного ландшафту у хмари, захисту хмарних середовищ. Дане бачення полягає в приєднанні зовнішніх сервісів (сервісів організацій-партнерів, державних органів: платформ закупівель, логістики та державних органів) до класичного розуміння хмари (приватні, громадські).

Зовнішні сервіси схожі по своїй організації з хмарними програмами, оскільки також контролюються сторонньою організацією, а користувачам цих сервісів залишається лише правильні у використанні. Відмінністю зовнішніх сервісів від хмарних додатків організацій є те, що хмарні програми самостійно визначають спосіб використання тих чи інших додатків, а зовнішні послуги реалізують жорстко прописану логіку взаємодії із сторонньою організацією. Проте рівень контролю для хмарних та зовнішніх сервісів часто ідентичний. Тому розумно розширювати бачення захисту хмарних сервісів саме таким способом (табл. 2) [16].

Багато компаній, запровадивши хмарну інфраструктуру, вже зараз стикаються з проблемою моментального впровадження комплексного підходу до захисту сервісних хмар. Для цього було виділено 8 ключових «контролів», які необхідно виконувати для базової хмари захисту.

1. Ідентифікація використовуваних хмар: аналіз мережного трафіку; використання програмного забезпечення Cloud Access Security Broker (CASB).

2. Відповідність вимогам регуляторів: перевірка надійності провайдера; реалізація необхідних контролів для захисту ресурсів у хмарі.

3. Захист доступу: посилена автентифікація (MFA – Multi-Factor Authentication), доступ довіреним пристроям.

4. Процеси ІБ у хмарі: оновлення процесів з урахуванням специфіки хмари.

5. Навчання працівників: внутрішні та зовнішні навчання; здавання сертифікацій.

6. Налаштування автоматизованих правил використання хмари: обмеження доступних для використання хмарних сервісів; розгортання хмарних ресурсів на основі шаблонів.

7. Автоматизація контролю ІБ у хмарі: автоматичне виявлення та блокування несанкціонованих змін у хмарних ресурсах.

8. Моніторинг ІБ: відправка подій з хмари у SIEM (Security Information and Event Management).

Опис, способи та інструменти усунення основних загроз хмарної інфраструктури

1. Недостатній рівень ІБ провайдера тягне за собою такі загрози забезпечення ІБ (ГІБ) хмарної інфраструктури:

a) загроза компрометації даних у хмарі через вразливу інфраструктуру провайдера;

b) загроза недоступності ресурсів та систем внаслідок порушення роботи хмарної платформи провайдера;

c) загроза невиконання вимог регуляторів;

d) необхідні дії для ОІБ – оцінка провайдера та хмарних сервісів, що їм надаються з урахуванням мети використання хмари та «чутливої» інформації, яка оброблятиметься у хмарі [17]. Для ОІБ можливе використання методики CSA (Cloud Security Alliance). Застосовні рівні фреймворку: інфраструктура.

2. Неконтрольований доступ до хмарних сервісів тягне у себе такі загрози:

• доступ колишніх співробітників до зовнішніх сервісів, що використовуються в компанії (електронні торгові майданчики, логістичні сис-

Таблиця 2

Підхід до захисту сервісних хмар

Рівні	Робітники	Приватні хмари	Публічні хмари	Внутрішня взаємодія
Доступ		Розмежування зон відповідальності у хмарі*		
	Контроль мережевого доступу	Контроль доступу до ресурсів		
	Контроль привілейованого доступу	Управління секретами		
		Інтегроване керування доступом*		
	Багатофакторна автентифікація	Керування доступом до API*		
Дані	Управління правами на доступ до даних (IRM)*		Шифрування даних у хмарі*	Віртуальні кімнати даних (VDR)
		Ідентифікація та класифікація даних		
	Захист від витоків даних			
	Контроль передачі даних у хмарі*			
Програми		Захист web-додатків		
		Захищена взаємодія сервісів у контейнерних середовищах*		
		Автоматизовані контролі ІБ у розробці / Безпека контейнерів (DevSecOps)		
Інфраструктура	Захист від шкідливого ПЗ			
	Управління мобільними пристроями	Захист платформи приватної хмари*	Оцінка провайдера*	
	Контроль «тіньових ІТ»			
	Просунутий захист робітників станцій	Захист інфраструктури	Автоматизація політик безпеки	
		Тестування на проникнення та BAS		
	Інтеграція з SOC			
Процеси ІБ	Управління ризиками ІБ	Тренінги та обізнаність		Політики та стандарти
	Аналіз потоків даних, бачення профілів користувачів	Регулярні вимоги		Управління інцидентами та проведення розслідувань
Позначення та скорочення:		* – Хмарні підходи (решта – класичні підходи) API – Application programming interface IRM – Information Rights Management VDR – Virtual Data Room DevSecOps – Development, Security and Operations BAS – Breach and Attack Simulation SOC – Security Operation Center		

теми, системи пошуку субпідрядників, хмарні послуги та ін.);

• відсутність контролю за зовнішніми сервісами, що використовуються;

• відсутність контролю над даними, переданими у зовнішні послуги;

• відсутність контролю доступу до зовнішніх сервісів;

• доступ із недовірених та вразливих пристроїв.

Необхідні дії для ОІБ такі:

• виявлення використовуваних хмарних сервісів, аналіз процесів їх використання та критичності;

• розробка регламенту контролю доступу користувачів до хмарних сервісів, що включає комплекс організаційних та технічних заходів;

• розробка рольової моделі та політик розмежування доступу до ресурсів;

• впровадження систем PIM/PAM (Privileged Identity Management/Privileged Access Management) для контролю дій адміністраторів;

• інтеграція хмари з MDM-системами (Master Data Management);

• тестування на проникнення.

Вибір вендора Indeed. Застосовні рівні фреймворку: доступ, дані.

3. Перехоплення контролю за ресурсами у хмарі тягне у себе такі загрози:

• складність інвентаризації активів у хмарі;

• відсутність зручних інструментів контролю за змінами, що вносяться з боку IT;

• відсутність розуміння процесів взаємодії активів у хмарі між собою та із зовнішнім світом;

• складність контролю процесу оновлення та розгортання активів;

• відсутність єдиної структурованої політики безпеки.

Необхідні дії для ГІБ такі:

• обстеження існуючих активів та «життєвого циклу» ресурсів у хмарі;

• розробка адаптованих під хмару процесів;

• використання систем управління ІБ громадських хмарних середовищ;

• впровадження систем контролю стану хмарних активів;

• створення екосистеми безпеки у приватних хмарах;

• розробка політик безпеки хмарних активів [18].

Проведений аналіз літературних джерел з тематики даної роботи, показує, що науці відомо сім основних напрямків втручання в хмарні сервіси SaaS, PaaS і IaaS:

− порушення конфіденційності під час використання хмарних технологій;

− порушення безпеки під час використання програмних інтерфейсів (API);

− порушення всередині компанії користувача;

− порушення цілісності систем віртуалізації;

− порушення правил аутентифікації, авторизації та аудиту, що тягне за собою втрату або витік інформації;

− порушення цілісності персональних даних, що надають доступ до необхідних сервісів;

− порушення стійкості внутрішньої інфраструктури системи [19].

Результатом спільної роботи організацій TCG і CSA, стосовно успішної організації безпеки хмарних систем на всіх її етапах роботи, стали сформовані рекомендації, які повинні бути враховані при укладенні договору між клієнтом і провайдером. Згідно рекомендаціям фахівців необхідно:

− використовувати технології шифрування для забезпечення збереження даних;

− захистити дані під час передавання, для цього потрібно використовувати надійні протоколи і алгоритми (наприклад TLS, IPsec і AES);

− організувати високий ступінь аутенфікації;

− ізолювати користувачів один від одного в тому плані, що дані і додатки одного клієнта повинні бути відокремлені від інших користувачів;

− провайдеру слідувати єдиній стратегії в нормативно-правовому аспекті;

− розробити документальні підтвердження на незаплановані події.

Виконання наданих порад дозволить вирішити безліч питань, пов'язаних з безпечним використанням хмарних сервісів.

Висновки. В умовах цифрової трансформації на ефективність бізнес-процесів впливають хмарні сервіси, які завдяки своїм перевагам є найбільш динамічно розвинутими у сфері інформаційних технологій. Авторами проаналізовано досвід роботи інженерів з інформаційної безпеки, що спеціалізуються в галузі проектування та впровадження засобів захисту сервісної хмарної інфраструктури, що дозволило обґрунтувати продуктивну типізацію та класифікацію застосовуваних хмар, визначити найбільш актуальні загрози, що зустрічаються в приватних та публічних хмарах, та способи їх усунення, виділити особливості поділу відповідальності між провайдером та користувачем хмарних сервісів (IaaS, PaaS, SaaS), а також обґрунтувати продуктивний підхід до забезпечення інформаційної безпеки у хмарі.

Список літератури:

1. Syantan G., Stephen Y., Arun-Balaji B. Attack Detection in Cloud Infrastructures Using Artificial Neural Network with Genetic Feature Selection. In Proceedings of the IEEE 14th International Conference on Dependable, Autonomic and Secure Computing, Athens, Greece, 12–15 August 2016; pp. 414–419.

2. Selamat N., Ali F. Comparison of malware detection techniques using machine learning algorithm. Indones. J. Electr. Eng. Comput. Sci. 2019, 16, 435.

3. Stefan H., Liakat M. Cloud Computing Security Threats And Solutions. J. Cloud Comput. 2015, 4, 1.

4. Venkatraman S., Mamoun A. Use of data visualisation for zero-day malware detection. Secur. Commun. Netw. 2018, 1–13.

5. Xue M., Yuan C., Wu H., Zhang Y., Liu W. Machine Learning Security: Threats, Countermeasures, and Evaluations. IEEE Access 2020, 8, 74720–74742.

6. Khan A. N., Fan M. Y., Malik A., Memon R. A. Learning from Privacy Preserved Encrypted Data on Cloud Through Supervised and Unsupervised Machine Learning. In Proceedings of the International Conference on Computing, Mathematics and Engineering Technologies, Sindh, Pakistan, 29–30 January 2019; pp. 1–5.

7. Khilar P., Vijay C., Rakesh S. Trust-Based Access Control in Cloud Computing Using Machine Learning. In Cloud Computing for Geospatial Big Data Analytics; Das, H., Barik, R., Dubey, H., Roy, D., Eds.; Springer: Cham, Switzerland, 2019; Volume 49, pp. 55–79.

8. Le Duc T., Leiva R. G., Casari P., Östberg, P. O. Machine Learning Methods for Reliable Resource Provisioning in Edge-Cloud Computing: A Survey. ACM Comput. Surv. 2019, 52, 1–39.

9. Lim S. Y., Kiah M. M., Ang T. F. Security Issues and Future Challenges of Cloud Service Authentication. Polytech. Hung. 2017, 14, 69–89.

10. Lin C., Lu H. Response to Co-resident Threats in Cloud Computing Using Machine Learning. In Proceedings of the International Conference on Advanced Information Networking and Applications, Caserta, Italy, 15–17 April 2020; Volume 926, pp. 904–913.

11. Al-Janabi S., Shehab A. Edge Computing: Review and Future Directions. REVISTA AUS J. 2019, 26, 368–380.

12. Alsolami E. Security threats and legal issues related to Cloud based solutions. Int. J. Comput. Sci. Netw. Secur. 2018, 18, 156–163.

13. Barona R., Anita M. A survey on data breach challenges in cloud computing security: Issues and threats. In Proceedings of the International Conference on Circuit, Power and Computing Technologies (ICCPCT), Paris, France, 17–18 September 2017; pp. 1–8.

14. Bhamare D., Salman T., Samaka M., Erbad A., Jain, R. Feasibility of Supervised Machine Learning for Cloud Security. In Proceedings of the International Conference on Information Science and Security, Jaipur, India, 16–20 December 2016; pp. 1–5.

15. Borylo P., Tornatore M., Jaglarz P., Shahriar N., Cholda P., Boutaba R. Latency and energy-aware provisioning of network slices in cloud networks. Comput. Commun. 2020, 157, 1–19.

16. Butt U. A., Mehmood M., Shah S. B. H., Amin R., Shaukat,M. W., Raza S. M., Piran M. J. A review of machine learning algorithms for cloud computing security. Electronics, 2020. 9(9), 1379.

17. Callara M., Wira P. User Behavior Analysis with Machine Learning Techniques in Cloud Computing Architectures. In Proceedings of the 2018 International Conference on Applied Smart Systems, Médéa, Algeria, 24–25 November 2018; pp. 1–6.

18. Carmo M., Dantas Silva F. S., Neto A.V., Corujo D., Aguiar, R. Network-Cloud Slicing Definitions for Wi-Fi Sharing Systems to Enhance 5G Ultra-Dense Network Capabilities. Wirel. Commun. Mob. Comput. 2019, 2019, 8015274.

19. Остапов С. Е. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Львів: «Новий Світ- 2000», 2020. – 678 с.

Prozur V.O. INTERVENTION IN CLOUD SERVICES: NEW CHALLENGES FOR INFORMATION SECURITY

The purpose of this article is to study cloud services, their capabilities and challenges. The article is devoted to the study of the issues of building and effective use of cloud services for building information security. The main principles of functioning of automated cloud services management systems are determined. The features of the proposed architecture are the use of portal technologies, automatic resource management and hybrid cloud infrastructure. Various research problems are defined from the point of view of distributed database storage, data security, heterogeneity and data visualization in cloud services. With the recent progress of computer technologies, the number of available cloud services is increasing day by day. However, excessive amounts of data create big problems for users. Meanwhile, cloud services provide a powerful environment for storing large amounts of data. Research results: describe approaches to protecting cloud services depending on the category of infrastructure used – private/public. A comparative analysis of the division of responsibility between the provider and the user of cloud services such as IaaS, PaaS, SaaS was conducted. The analysis showed that companies provide protection for all levels of cloud infrastructure independently when using a private cloud service. When using a public cloud service, the company has less control over protection, which allows saving money on service specialists, but deprives the ability to make significant changes to the current infrastructure to comply with regulatory requirements. The practical significance of the research is confirmed by the definition of a set of practical recommendations for eliminating the main threats to cloud infrastructure by using protection tools of different classes, examples of which are presented in the work.

Key words: *cloud computing, security tools, databases, hybrid cloud infrastructures, public cloud service.*