УДК 004.056.5
DOI: https://doi.org/10.36994/2788-5518-2024-01-07-04

ОГЛЯД МЕТОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ХМАРНОМУ СЕРЕДОВИЩІ

***Борисенко О. С.**, Відкритий міжнародний університет розвитку людини «Україна», Київ, Україна. https://orcid.org/0009-0001-3738-5878, alekborysenko@gmail.com*

***Тимошенко А. Г.**, к.т.н., доц., Відкритий міжнародний університет розвитку людини «Україна», Київ, Україна. https://orcid.org/0000-0003-0954-3186, timoshag@i.ua*

***Анотація.** З розвитком інформаційних технологій і популяризацією хмарних сервісів усе більше компаній та індивідуальних користувачів зберігають і обробляють дані у хмарі. Ця тенденція забезпечує доступність даних, гнучкість у масштабуванні ресурсів і зниження витрат на IT-інфраструктуру. Проте виникають виклики щодо захисту персональних даних у хмарному середовищі.*

У статті розглядаються сучасні ризики зберігання й обробки персональних даних у хмарі та рекомендації для їх мінімізації. Основні загрози стосуються витоку даних, що може призвести до несанкціонованого доступу та розкриття конфіденційної інформації, а також проблем із дотриманням регуляторних вимог.

Рекомендації передбачають використання надійних методів контролю доступу, шифрування даних, регулярну оцінку вразливостей і тестування на проникнення. Відмічається важливість забезпечення відповідності вимогам таких нормативних актів, як GDPR, HIPAA та CCPA, через регулярні аудити та чіткі політики управління даними.

Особлива увага приділяється безпеці API, які можуть бути вразливими до атак. Для захисту API рекомендується безпечне кодування, регулярний моніторинг і автентифікація.

Упровадження надійного контролю доступу, включно з принципом мінімальних привілеїв, мультифакторною автентифікацією, рольовою моделлю доступу та безперервним моніторингом, є ключовим елементом стратегії захисту. Шифрування даних під час передачі та зберігання, використання TLS/SSL-протоколів і серверного шифрування від хмарних провайдерів допомагає забезпечити конфіденційність і цілісність даних.

Стаття підкреслює важливість практик безпечної розробки, регулярних аудитів і моніторингу, а також відповідності регуляціям щодо захисту даних. Упровадження цих заходів дає змогу організаціям ефективно захищати персональні дані у хмарному середовищі, мінімізувати ризики й відповідати законодавчим вимогам.

***Ключові слова:** захист персональних даних, контроль доступу, шифрування, аудит безпеки.*

OVERVIEW OF PERSONAL DATA PROTECTION METHODS IN THE CLOUD ENVIRONMENT

***Oleksandr Borysenko,** Open International University of Human Development "Ukraine", Kyiv, Ukraine. https://orcid.org/0009-0001-3738-5878, alekborysenko@gmail.com*

***Anatolii Tymoshenko,** Ph.D., Ass. Prof., Open International University of Human Development "Ukraine", Kyiv, Ukraine. https://orcid.org/0000-0003-0954-3186, timoshag@i.ua*

***Abstract.** With the advancement of information technology and the popularization of cloud services, more and more companies and individual users are storing and processing data in the cloud. This trend ensures data accessibility, flexibility in resource scaling, and reduced IT infrastructure costs. However, challenges arise regarding the protection of personal data in the cloud environment.*

This article examines the modern risks of storing and processing personal data in the cloud and provides recommendations for minimizing these risks. Major threats include data breaches, which can lead to unauthorized access and disclosure of confidential information, as well as compliance issues with regulatory requirements.

The recommendations include using reliable access control methods, data encryption, regular vulnerability assessments, and penetration testing. It is crucial to ensure compliance with regulations such as GDPR, HIPAA, and CCPA through regular audits and clear data management policies.

Special attention is given to the security of APIs, which can be vulnerable to attacks. To protect APIs, secure coding, regular monitoring, and authentication are recommended.

Implementing robust access control, including the principle of least privilege, multi-factor authentication, role-based access control, and continuous monitoring, is a key element of the protection strategy. Data

encryption during transmission and storage, using TLS/SSL protocols, and server-side encryption from cloud providers help ensure data confidentiality and integrity.

The article emphasizes the importance of secure development practices, regular audits and monitoring, and regulatory compliance for data protection. Implementing these measures allows organizations to effectively protect personal data in the cloud environment, minimize risks, and meet legislative requirements.

Key words: *personal data protection, access control, encryption, security audit.*

Вступ

Останнім часом дуже зросла популярність хмарних сервісів для зберігання й обробки даних у хмарному середовищі. Хмари використовуються як індивідуальними користувачами, так і великими компаніями. Цей підхід несе багато переваг: зниження витрат на IT-інфраструктуру, гнучкість у масштабуванні ресурсів, зручність використання, доступ до даних з будь-якої точки світу. Однак разом із цими перевагами постають серйозні питання щодо захисту персональних даних у хмарному середовищі. У цій статті розглядаються основні ризики й методи захисту персональних даних у хмарі.

Метою дослідження є огляд і класифікація сучасних ризиків зберігання й обробки персональних даних у хмарному середовищі, а також вироблення рекомендацій для уникнення або зменшення цих ризиків.

Виконання досліджень

Насамперед розглянемо загальні проблеми, пов'язані зі зберіганням даних у хмарному середовищі, і можливі загрози. Однією з основних загроз є виток даних. Вони можуть призвести до несанкціонованого доступу та розкриття конфіденційної інформації, від особистих даних до фінансових записів. Вплив є не тільки фінансовим, але й поширюється на репутаційні втрати, втрату довіри клієнтів і можливі юридичні наслідки.

Найкращою стратегією запобігання буде:

а) використання надійних методів контролю доступу, щоб обмежити кількість осіб з доступом до конфіденційних даних;

б) упровадження шифрування для захисту даних як під час зберігання, так і під час передачі;

в) регулярне проведення оцінки вразливостей і тестування на проникнення для виявлення й усунення потенційних слабких місць.

Іншою потенційною проблемою може бути проблема з регуляторними органами. Різні регіони та галузі мають різні вимоги щодо захисту даних, такі як GDPR у Європі, HIPAA в охороні здоров'я та CCPA у Каліфорнії. Недотримання цих вимог може призвести до суворих штрафів та юридичних дій.

Найкращою стратегією запобігання буде:

а) слідкувати за оновленням відповідних нормативних документів, забезпечувати, щоб заходи безпеки відповідали їх вимогам;

б) проводити регулярні аудити відповідності для виявлення та вирішення потенційних проблем;

в) встановити чіткі політики управління даними для забезпечення належного оброблення персональних даних.

Ще однією важливою проблемою є безпека API. Багато додатків використовують API для з'єднання з хмарними сервісами. Незахищені API можуть бути використані зловмисниками, що призводить до несанкціонованого доступу, маніпуляції даними та навіть порушення роботи сервісу.

Найкращою стратегією запобігання буде:

а) використання безпечних практик кодування під час розробки API;

б) регулярна перевірка та моніторинг використання API для виявлення підозрілої активності;

в) використання механізмів автентифікації, такі як ключі API або OAuth, для контролю доступу до API.

Розглянемо більш детально впровадження надійного контролю доступу. Його можна розділити на такі складові:

а) принцип мінімальних привілеїв, який надає такий рівень доступу користувачам і додаткам, який є мінімально необхідним для виконання їхніх завдань. Для його впровадження слід призначати ролі та дозволи на основі посадових обов'язків і регулярно переглядати й оновлювати надані дозволи, щоб вони відповідали зміні ролей і обов'язків;

б) мультифакторна автентифікація (MFA), яка надає такий рівень автентифікації, що виходить за межі імені користувача та пароля, вимагаючи додаткові форми перевірки. MFA потрібно впроваджувати для всіх користувачів, які мають доступ до конфіденційних даних або критичних систем;

в) рольова модель доступу (RBAC), яка надає дозволи на основі робочих ролей користувачів, забезпечуючи доступ лише до ресурсів, які стосуються їхніх обов'язків. Для її впровадження потрібно визначити ролі з конкретними дозволами на основі тих функцій, які вони виконують, та регулярно переглядати й оновлювати політики RBAC, щоб вони відображали організаційні зміни;

г) безперервний моніторинг, який забезпечує видимість дій користувачів у реальному часі, що дає змогу швидко виявляти несанкціонований доступ або підозрілу поведінку. Для його впровадження

потрібно використовувати інструменти управління інформаційною безпекою та подіями (SIEM) для моніторингу дій користувача на основі логів і подій та налаштовувати сповіщення для незвичайної або потенційно шкідливої активності.

Ще одним важливим аспектом захисту даних є їх шифрування. Воно може відбуватися під час передачі або зберігання даних.

Для шифрування під час передачі даних використовуються протоколи TLS та SSL. Протокол Transport Layer Security (TLS) є стандартним протоколом для забезпечення безпеки комунікацій у комп'ютерній мережі. Він забезпечує конфіденційність і цілісність даних, що передаються між системами. Сертифікати Secure Sockets Layer (SSL) є криптографічними ключами, які ініціюють рукостискання TLS, встановлюючи безпечне з'єднання. Вони є важливими для шифрування даних під час передачі.

Шифрування під час зберігання може бути надане хмарним провайдером. Більшість із них пропонують серверне шифрування (server side encryption – SSE), де вони автоматично шифрують дані перед зберіганням їх у своїй інфраструктурі. Хмарні провайдери керують ключами шифрування, що забезпечує зручне рішення для багатьох користувачів.

Шифрування також може відбуватися на стороні клієнта. Організації можуть вибрати управління своїми ключами шифрування, додаючи додатковий рівень контролю. У разі шифрування на стороні клієнта дані шифруються на стороні клієнта до того, як вони потрапляють у хмару, забезпечуючи захист від кінця до кінця.

Шифрування даних забезпечує конфіденційність, а отже, тільки авторизовані сторони можуть отримувати доступ і розуміти дані. Шифрування запобігає несанкціонованій зміні даних, зберігаючи їх точність і цілісність. Багато нормативних документів щодо захисту даних вимагають або рекомендують шифрування як захід для захисту особистої та конфіденційної інформації.

Одним із важливих аспектів є дотримання практик безпечної розробки. До них належить валідація вхідних даних. Їх перевірка й очищення, щоб запобігти поширеним вразливостям, таким як SQL-ін'єкції та міжсайтові скрипти (XSS). Упровадження надійних механізмів аутентифікації та авторизації, а також розробка надійних механізмів обробки помилок, щоб запобігти розкриттю конфіденційної інформації у повідомленнях про помилки. Критичним є постійне навчання з безпеки для команд розробників, щоб вони були в курсі новітніх загроз і найкращих практик. Навчальні програми повинні бути адаптовані відповідно до ролей розробників, зосереджені на специфічних проблемах безпеки, з якими вони можуть зіткнутися. Потрібні регулярні процеси перевірки коду. Ручні перевірки коду слід доповнювати автоматизованими інструментами, які можуть виявляти поширені проблеми безпеки, такі як інструменти статичного аналізу. Інтеграція планування реагування на інциденти в життєвий цикл розробки забезпечує швидке реагування на будь-які інциденти безпеки.

Одну з ключових ролей у захисті інформації відіграє регулярний аудит та моніторинг. У ньому можна виділити такі напрями:

а) безперервний моніторинг, який передбачає спостереження за активністю в хмарному середовищі в режимі реального часу. Автоматизовані інструменти можуть аналізувати моделі поведінки й піднімати тривогу в разі виявлення відхилень від норми. Інтеграція із системами управління інформаційною безпекою та подіями (SIEM) централізує дані логів для аналізу, кореляції та звітності;

б) аудити та оцінки. Регулярно заплановані аудити, як внутрішні, так і зовнішні, забезпечують систематичний огляд заходів безпеки та конфігурацій. Періодичні оцінки виявляють і усувають потенційні вразливості в хмарній інфраструктурі. Імітація кібератак допомагає оцінити ефективність заходів безпеки та виявити області для покращення;

в) відповідність нормативним документам. Організації, що підлягають певним регуляціям, повинні проводити аудити для підтвердження дотримання нормативних вимог, вести записи про практики безпеки та зберігати результати аудитів;

г) використання систем виявлення вторгнень (IDS). Ці інструменти постійно здійснюють моніторинг мережевої або системної активності на наявність шкідливої діяльності або порушень політики безпеки. Автоматизовані інструменти можуть оптимізувати рутинні завдання з безпеки, даючи змогу командам безпеки зосередитися на більш складних загрозах; автоматизовані системи оповіщення забезпечують швидке інформування про інциденти безпеки відповідного персоналу для розслідування й реагування;

ґ) регулярний моніторинг. Раннє виявлення інцидентів безпеки дає змогу швидко реагувати, мінімізуючи потенційні збитки. Безперервний моніторинг допомагає організаціям залишатися гнучкими перед новими загрозами кібербезпеки. Детальні логи з безперервного моніторингу дають змогу проводити ретельний форензичний аналіз після інциденту безпеки, допомагаючи зрозуміти природу й обсяг атаки.

Дані в разі зберігання й обробки повинні відповідати вимогам щодо захисту даних. До цих вимог належать:

а) нормативні документи GDPR, HIPAA, CCPA. Загальний регламент захисту даних (GDPR) зосереджується на конфіденційності та захисті персональних даних громадян Європейського Союзу.

Закон про переносимість і відповідальність медичного страхування (HIPAA) стосується безпеки та конфіденційності медичної інформації в галузі охорони здоров'я. Каліфорнійський закон про конфіденційність споживачів (CCPA) надає права на конфіденційність мешканцям Каліфорнії, вимагаючи від бізнесу розкривати практики щодо даних;

б) чіткі правила, що визначають місцезнаходження персональних даних в організації, спосіб їх обробки, процеси отримання й управління згодою користувачів на обробку даних, а також механізми реалізації прав осіб, таких як право на доступ та право бути забутим;

в) оцінка ризиків впливу на захист даних за процедурою DPIA;

г) шифрування даних для захисту конфіденційності персональних даних як під час передачі, так і під час зберігання, та псевдонімізація, тобто заміщення ідентифікуючої інформації псевдонімами для зменшення ризику, пов'язаного з обробкою персональних даних;

ґ) виявлення та своєчасне повідомлення про витоки даних із дотриманням регуляторних вимог щодо повідомлення; встановлення протоколів комунікації для інформування постраждалих осіб та відповідних органів про витоки даних;

д) призначення відповідальних за захист даних (DPO) для надання експертних порад із питань захисту даних і забезпечення узгодження з відповідними нормами; також DPO слугує контактною особою для регуляторних органів та суб'єктів даних із питань захисту даних;

е) проведення регулярних внутрішніх аудитів для оцінки та забезпечення постійної відповідності вимогам щодо захисту даних; залучення зовнішніх аудиторів для надання незалежної оцінки зусиль з відповідності.

є) дотримання принципів конфіденційності за дизайном, у процесі розробки, які забезпечують наявність функцій конфіденційності за замовчуванням. Також потрібно збирати й обробляти тільки ті дані, які необхідні для виконання поставленого завдання, дотримуючись принципу мінімізації даних.

Завдяки впровадженню захищених практик розробки та дотриманню суворих вимог щодо захисту даних організації можуть створювати додатки, які не тільки відповідають законодавчим вимогам, але й пріоритетно ставляться до конфіденційності та безпеки персональних даних, з якими вони працюють. Ці практики сприяють формуванню культури безпеки й демонструють зобов'язання щодо захисту конфіденційної інформації протягом усього життєвого циклу додатка.

Висновки

Упровадження хмарних технологій приносить значні переваги, такі як доступність, гнучкість і зниження витрат, але водночас створює серйозні виклики у сфері безпеки даних. У цій статті було розглянуто основні ризики, пов'язані зі зберіганням і обробкою персональних даних у хмарному середовищі, а також запропоновано рекомендації для їх мінімізації.

Однією з ключових загроз є витік даних, що може призвести до значних фінансових втрат, пошкодження репутації та юридичних наслідків. Для запобігання витокам даних рекомендується впровадження надійних методів контролю доступу, шифрування даних і регулярного тестування на проникнення. Важливим є також дотримання регуляторних вимог, таких як GDPR, HIPAA та CCPA, через проведення регулярних аудитів і забезпечення відповідності заходів безпеки.

Література

1. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, 28 (3), 583–592.
2. Rittinghouse, J.W., & Ransome, J.F. (2016). *Cloud Computing: Implementation, Management, and Security*. CRC Press.
3. Hwang, K., & Li, D. (2010). Trusted cloud computing with secure resources and data coloring. *IEEE Internet Computing*, 14 (5), 14–22.
4. Pearson, S. (2013). Privacy, Security and Trust in Cloud Computing. In *Privacy and Security for Cloud Computing* (pp. 3–42). Springer, London.
5. Cloud Security Alliance (CSA). (2021). Security Guidance for Critical Areas of Focus in Cloud Computing v4.0.
6. Fernandes, D.A.B., Soares, L.F.B., Gomes, J.V., Freire, M.M., & Inácio, P.R.M. (2014). Security issues in cloud environments: a survey. *International Journal of Information Security*, 13 (2), 113–170.

References

1. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, 28 (3), 583–592.
2. Rittinghouse, J.W., & Ransome, J.F. (2016). *Cloud Computing: Implementation, Management, and Security*. CRC Press.
3. Hwang, K., & Li, D. (2010). Trusted cloud computing with secure resources and data coloring. *IEEE Internet Computing*, 14 (5), 14–22.
4. Pearson, S. (2013). Privacy, Security and Trust in Cloud Computing. In *Privacy and Security for Cloud Computing* (pp. 3–42). Springer, London.
5. Cloud Security Alliance (CSA). (2021). Security Guidance for Critical Areas of Focus in Cloud Computing v4.0.
6. Fernandes, D.A.B., Soares, L.F.B., Gomes, J.V., Freire, M.M., & Inácio, P.R.M. (2014). Security issues in cloud environments: a survey. *International Journal of Information Security*, 13 (2), 113–170.