УДК 004.81

О. П. Войтович
Є. В. Радченко
І. Ю. Пилявець

АКТУАЛЬНІСТЬ ВИКОРИСТАННЯ ЛОКАЛЬНИХ ІНСТРУМЕНТІВ ПІДТРИМКИ АУДИТУ

Вінницький національний технічний університет

Анотація

Розглянуто переваги та недоліки використання хмарних технологій в процесі аудиту. Проаналізовано сучасні рішення в сфері підтримки аудиту в умовах роботи з конфіденційною інформацією та інформацією з обмеженим доступом. Використання хмарних технологій дозволяє не тільки зменшити навантаження на локальне апаратне забезпечення підприємства чи організації, що проводить аудит, а й спростити процес передачі інформації. Оскільки сучасні інструменти підтримки аудиту мають велику кількість функцій для спрощення та покращення процесу аудиту, їх використання здається очевидним рішенням. Проте з'являються ризики витоків інформації, що розміщена в хмарних сервісах, юридичні проблеми а також питання довіри до постачальника послуг.

Ключові слова: аудит, інформаційна безпека, автоматизація, кібербезпека, аудит відповідності, моніторинг, аналіз даних, виявлення загроз, хмарні сервіси, конфіденційна інформація.

Abstract

The advantages and disadvantages of using cloud technologies in the audit process are considered. Modern solutions in the field of audit support in the conditions of working with confidential information and information with limited access are analyzed. The use of cloud technologies allows not only to reduce the load on the local hardware of the enterprise or organization conducting the audit, but also to simplify the process of transferring information. Since modern audit support tools have a large number of features to simplify and improve the audit process, using them seems like an obvious solution. However, there are risks of leakage of information hosted in cloud services, legal problems, as well as issues of trust in the service provider.

Keywords: audit, information security, automation, cybersecurity, compliance audit, monitoring, data analysis, threat detection, cloud services, confidential information.

Вступ

З плином часу питання кібербезпеки та захисту інформації стають тільки гострішими. Враховуючи умови гібридної війни, можна припустити, що інформація стає стратегічною ціллю ворога. Таким чином, зростає потреба в проведенні аудитів інформаційної безпеки. Водночас, будь-який аудит має значний недолік – довготривалість процесу. Через велику кількість інформації, що потребує обробки та значну кількість вимог і стандартів, процес проведення аудиту інформаційної безпеки може розтягнутись на декілька місяців. В умовах підвищеного ризику кібератак, витоків інформації та інших інцидентів, подібні затримки можуть мати руйнівні наслідки. Метою даної роботи є аналіз існуючих інструментів підтримки аудиту в контексті захисту інформації від витоків.

Результати дослідження

Незважаючи на популярність хмарних сервісів, з точки зору захисту інформації, цей підхід має певні недоліки. В основному вони полягають в можливих вразливостях, що можуть з'явитись як на стороні постачальника послуг, так і на стороні споживача, адже процес передачі інформації сам по собі збільшує ризик витоку[1]. Звісно, інформація в стані переміщення є надзвичайно вразливою, проте варто враховувати також і той факт що хмарні сервіси також можуть бути цілями для атак та джерелами витоків.

Іншим, доволі значним недоліком, залишається відсутність контрактних відносин між споживачем та постачальником, які регламентують процес збереження, передачі та обробки інформації, такі питання як відповідальність за витік даних та компенсація завданих збитків. Припустімо, що в процесі аудиту існує необхідність передачі даних з корпоративної мережі підприємства, що проходить аудит інформаційної безпеки до корпоративної мережі підприємства, що надає послуги з проведення аудиту. При використанні захищених методів передачі даних, ризики зводяться до мінімальних[2], проте, як показує практика, доволі часто в критичних процесах, що обробляють чутливу інформацію, використовуються менш надійні засоби передачі даних – незахищена пошта, хмарні сховища з відкритим доступом, портативні носії інформації, тощо [3]

Аналогічним чином, більшість компаній, що належать до великого бізнесу та вкладають значні кошти в забезпечення інформаційної безпеки, заключають контракти то договори зі сторонніми організаціями, що надають послуги хмарних сервісів. Для прикладу, при заключенні договору з компанією Microsoft на постачання ліцензованого програмного забезпечення, що надає послуги поштового сервісу, договір між компаніями уточнює, що Microsoft несе відповідальність за витоки інформації, що відбуваються на стороні хмарного сервісу[4].

З іншого боку, якщо для передачі інформації використовуються сервіси, що не мають юридичних зобов'язань перед підприємством, за виключенням звичайних умов обслуговування, які застосовуються до фізичних осіб, відповідальність постачальника послуг за витік інформації може бути значно меншою. Для прикладу, Google гарантує безпеку даних, що зберігаються на хмарному сервісі «Google Drive», проте в умовах використання вони заявляють що в окремих випадках можуть отримати доступ до ваших даних та навіть надати їх стороннім особам[5].

В умовах аудиту інформаційної безпеки важливо розуміти ризики, пов'язані з використанням хмарних ресурсів. Мова йде не лише про технічні вразливості, а й аспекти організаційного та юридичного підходу до питання обробки, зберігання та передачі інформації. Так, навіть в умовах використання найбільш захищеного хмарного сервісу, відсутність чіткого розмежування зон відповідальності та наслідків витоків інформації за допомогою юридично затверджених договорів про нерозповсюдження інформації збільшує ризики при використанні даного хмарного сервісу[6].

Враховуючи ризики використання хмарних сервісів, розміщення програмних засобів в локальній мережі зберігає свою актуальність, не дивлячись на такі недоліки як мала обчислювальна потужність, необхідність покриття витрат на встановлення програмного та апаратного забезпечення, відсутність провідних технологій, що впроваджуються в певних хмарних сервісах.

З іншого боку, такий підхід має і свої переваги. Зокрема, зниження ризиків витоку інформації. Оскільки вся інформація зберігається в локальній мережі підприємства, та не передається за її межі, кількість можливих вразливостей зменшується. Використовується менша кількість каналів зв'язку та сторонніх сервісів, що можуть мати власні властивості. За необхідності обробки інформації аудиторами, можна допустити їх до локальної мережі підприємства з обмеженим доступом. Це дозволить зменшити ризики, не компрометуючи процес проведення аудиту.

До інших переваг інструментів підтримки аудиту, розміщених локально, можна віднести гнучкість. На відміну від великих рішень, що змушують підприємства малого та середнього бізнесу вносити корективи у власні інформаційні системи, програмне забезпечення, ро розробляється під конкретні вимоги підприємства, може бути адаптовано. Аналогічним чином, варто звернути увагу на питання швидкодії, враховуючи відсутність процесу передачі інформації, а також повний контроль над доступом до інформації

Висновки

Хмарні сервіси мають значний потенціал в будь-якій сфері, що стосується обробки інформації. Проте, в той же час, більш традиційні локальні рішення не втрачають актуальності через такі переваги як адаптивність, зниження ризиків шляхом збереження інформації всередині локальної мережі підприємства, більший контроль над процесом, тощо. Проте, при виборі конкретних інструментів підтримки аудиту необхідно враховувати потреби поточного процесу, адже кожен з розглянутих підходів має власні переваги та недоліки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Analysis of modern cloud services to ensure cybersecurity / Y. Pedchenko та ін. Procedia Computer Science. 2022. Т. 207. С. 110–117. URL: https://doi.org/10.1016/j.procs.2022.09.043 (дата звернення: 02.12.2024).
2. Schneider M. Secure Automated File Exchange (SAFE) – Enabling More Efficient Transfers of Sensitive Data. International Journal of Population Data Science. 2020. Т. 5, № 5. URL: https://doi.org/10.23889/ijpds.v5i5.1599 (дата звернення: 02.12.2024).
3. A systematic analysis of failures in protecting personal health data: A scoping review / J. Pool та ін. International Journal of Information Management. 2024. Т. 74. С. 102719. URL: https://doi.org/10.1016/j.ijinfomgt.2023.102719 (дата звернення: 02.12.2024).
4. Microsoft. Data retention, deletion, and destruction in Microsoft 365 - Microsoft Service Assurance. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-retention-deletion-and-destruction-overview (дата звернення: 02.12.2024).
5. Google. Google Terms of Service – Privacy & Terms – Google. Privacy & Terms – Google. URL: https://policies.google.com/terms#toc-content (дата звернення: 02.12.2024).
6. Realities of Academic Data Sharing (RADS) Initiative Public-Access Data Management and Sharing (DMS) Activities, v3 / W. Kozlowski et al. Association of Research Libraries, 2023. URL: https://doi.org/10.29242/radsdmsactivities2023 (date of access: 02.12.2024).

Науковий керівник: ***Войтович Олеся Петрівна*** — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця,
e-mail: voytovych.op@gmail.com

Радченко Євгеній Валентинович — студент групи 1БС-23М, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця,
e-mail: jenya.radchenko@gmail.com.

Пилявець Ігор Юрійович — студент групи 1БС-23М, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця,
e-mail: igormorozov920@gmail.com.

Supervisor: ***Voytovych Olesya Petrovna*** — Cand. Sc., Associate Professor of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: voytovych.op@gmail.com

Radchenko Yevhenii V.— student of group 1BS-23M, faculty of information technologies and computer engineering, Vinnytsia National Technical University, email: jenya.radchenko@gmail.com.

Pyliavets Ihor Y.— student of group 1BS-23M, faculty of information technologies and computer engineering, Vinnytsia National Technical University, email: igormorozov920@gmail.com.