УДК 316.776:004.58

Дослідження методів захисту та розробка рекомендацій щодо створення захищених каналів зв’язку та забезпечення безпеки хмарних сховищ даних

Костянтин Дема[0009-0002-5349-0384]
Андрій Аносов[0000-0002-2973-6033]

Київський столичний університет імені Бориса Грінченка, Україна

Анотація. Ці тези представляють дослідження та порівняння методів захисту щодо створення захищених каналів зв'язку та забезпечення безпеки хмарних сховищ даних. На її основі також будуть представленні рекомендації щодо їх комбінаторного впровадження.
Ключові слова: сховище даних, інформаційна безпека, захист даних, шифрування, автентифікація, інцидент.

Investigation of Methods of Protection and Development of Recommendations for the Effective Creation of Stolen Channels, Communication and Security of Dangerous Data Sources

Kostiantyn Dema[0009-0002-5349-0384]
Andrii Anosov[0000-0002-2973-6033]

Borys Grinchenko Kyiv Metropolitan University, Ukraine

Abstract. This paper presents the research and improvement of methods for protecting the stolen channels, connecting them, and ensuring the safety of data storage facilities. On this basis, recommendations will also be presented for their combinatorial implementation.
Keywords: data storage, information security, data protection, encryption, authentication, incident.

Вступ

Сучасний розвиток хмарних сервісів відкрив широкі можливості для розвитку бізнесу, освіти, науки та приватних користувачів, однак одночасно створив нові вектори для кібератак і несанкціонованого доступу до даних.

У сучасних умовах стрімкого розвитку хмарних сховищ даних особливої актуальності набувають питання інформаційної безпеки та захисту даних. Для досягнення цього використовуються сучасні методи шифрування (encryption), автентифікації та контролю доступу, які дозволяють мінімізувати ризики несанкціонованого доступу та втрати критично важливої інформації у хмарному середовищі.

Захист каналів зв’язку є ключовим елементом у забезпеченні інформаційної безпеки, адже саме під час передачі даних відбувається найбільша кількість атак — від перехоплення трафіку до підміни інформації. Тому дослідження методів

криптографічного захисту, автентифікації та протоколів безпечного обміну є необхідною умовою створення надійних систем зв'язку.

Методи та моделі

Насамперед потрібно сказати що дослідження методів захисту річ не нова, і на цю тему існують багато документацій що дозволяють передбачити виникнення інцидентів на багатьох рівнях передачі даних, в тому числі і при передачі та/або їх збереження у хмарних середовищах.

Рис. 1 Основний шлях виникнення інцидентів

Опираючись на таку основу експерти розрізняють наступні основні методи захисту інформації безпосередньо під час їх передачі по каналам зв'язку:

- Шифрування даних
- Цифрові підписи
- Хешування
- Протоколи захищеного обміну

Та під час їх зберігання у хмарних сховищах:

- Використання протоколів HTTPS, TLS/SSL
- Управління доступом і автентифікація
- Ідентифікація та керування користувачами
- Забезпечення цілісності та відмовостійкості
- Резервне копіювання (backup) і реплікація даних — захист від втрати інформації.

Результати

В результаті можна створити таблицю основних шляхів захисту для їх легшого порівняння переваг та недоліків та короткого опису.

З результату таблиці ми бачимо що кожен метод має низку переваг та недоліків і навіть ідеальний варіант для одної системи – середовища може бути неприйнятним для іншого, і головна ідея створення таких систем є в комбінованому, індивідуальному підході. Зі всього цього можна зробити висновок, що ефективна система забезпечення безпеки даних неможлива при використанні лише одного окремого підходу. Кожен із методів має свої переваги та обмеження: криптографічні засоби гарантують конфіденційність, але не захищають від внутрішніх загроз; протоколи безпечного обміну забезпечують надійність передачі, проте не контролюють доступ до збережених даних; а резервне копіювання лише мінімізує наслідки інцидентів, але не запобігає їм.

Таблиця 1. Порівняльна характеристика методів захисту

Метод	Опис	Переваги	Недоліки
Шифрування даних	Перетворює інформацію у зашифрований формат, недоступний для сторонніх осіб.	Високий рівень конфіденційності; ефективно при передачі та зберіганні; широка підтримка протоколів (AES, RSA).	Вимагає обчислювальних ресурсів; можливість втрати ключів.
Цифрові підписи	Підтверджують справжність відправника і цілісність даних.	Гарантують автентичність; неможливо підробити без приватного ключа; підходить для юридично значущих документів.	Потребує інфраструктури відкритих ключів (PKI); може збільшити розмір переданих даних.
Хешування	Формує унікальний код для контролю цілісності інформації.	Простота реалізації; висока швидкість перевірки цілісності; використовується в аутентифікації.	Не забезпечує конфіденційність
Протоколи захищеного обміну (SSL/TLS, SSH, IPsec)	Забезпечують шифрування та автентифікацію під час передачі даних мережею.	Високий рівень безпеки; захищають від перехоплення трафіку; автоматична інтеграція у браузерах.	Залежність від правильного налаштування сертифікатів; зниження швидкодії при великому навантаженні.

Найвищий рівень безпеки досягається шляхом комбінації кількох методів одночасно, що дозволяє компенсувати недоліки кожного з них. Зокрема, поєднання шифрування, протоколів захищеного обміну, багатофакторної автентифікації та регулярного резервного копіювання створює багаторівневу систему захисту, здатну забезпечити цілісність, конфіденційність і доступність даних як під час їх передачі каналами зв’язку, так і при зберіганні у хмарному середовищі.

Обговорення

Результати досліджень є доволі перспективними з огляду на постійний розвиток у сфері шифрування даних - очікується поширення алгоритмів криптографії, здатних протистояти обчислювальним можливостям квантових комп’ютерів. Це дозволить гарантувати довгостроковий захист критичної інформації. Також цифрові підписи та

технології автентифікації набуватимуть більшої гнучкості через використання блокчейн-рішень, які забезпечують прозорість і неможливість підробки записів, а у напрямку керування доступом і автентифікації передбачається ширше впровадження біометричних технологій, а також архітектури Zero Trust, яка передбачає постійну перевірку кожного запиту незалежно від його джерела.

Порівняння з роботами інших авторів підтверджує, що саме гібридні рішення, які поєднують актуальні ідеї та можливості нових систем та ПК, дають найкращий баланс між продуктивністю і рівнем безпеки.

Висновки

Сучасні системи безпеки мають базуватися на комплексному підході, який поєднує криптографічні методи, протоколи захищеного обміну, автентифікацію та резервне копіювання. Така інтеграція дозволяє забезпечити одночасно конфіденційність, цілісність і доступність даних як під час передачі, так і при зберіганні у хмарних середовищах.

Основною тенденцією розвитку у сфері захисту хмарних сховищ є підвищення рівня автоматизації та інтелектуалізації засобів безпеки. Зокрема, активно впроваджуються рішення на основі штучного інтелекту та машинного навчання для моніторингу, виявлення аномалій і прогнозування можливих кібератак. Водночас розвиваються постквантові криптографічні алгоритми, орієнтовані на мінімізацію ризиків у розподілених середовищах. Прогнозується, що у майбутньому головними проблемними аспектами стануть зростання кількості цільових атак на хмарні сервіси, ризики, пов’язані з людським фактором, а також забезпечення сумісності різних систем захисту у гібридних хмарних інфраструктурах. Тому подальші дослідження мають бути спрямовані на створення адаптивних, самонавчальних систем кібербезпеки, здатних динамічно реагувати на нові загрози в реальному часі.

Джерела

1. ВСП "ОТФК ОНТУ", Відділення Комп`ютерних систем. Аналіз та практична реалізація методів захисту каналів зв’язку пристроїв клавіатурного введення, 2022. Протасенко Олександр Ігорович. https://card-file.ontu.edu.ua/items/25f19ce7-d334-4348-a390-2d3455b6a680

2. Складанний, П., Костюк, Ю., Мазур, Н., & Пітайчук, М. (2025). Дослідження характеристик та продуктивності протоколів доступу до хмарних обчислювальних середовищ на основі універсального тестування. Телекомунікаційні та інформаційні технології, 1(86), 61–74. https://doi.org/10.31673/2412-4338.2025.014649

3. Дослідження захищеності каналів зв’язку на основі технології розширення спектру / Research security of communication channels based on spread-spectrum technology С.Родін, 2015 https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/3752/rodins.pdf

4. Костюк, Ю., Хорольська, К., Бебешко, Б., Довженко, Н., Коршун, Н., & Пазинін, А. (2025). Інструментальні засоби забезпечення інформаційної безпеки від прихованих загроз в інфраструктурі хмарних обчислень. Кібербезпека: освіта, наука, техніка, 4(28), 633–655. https://doi.org/10.28925/2663-4023.2025.28.857

5. Дослідження методів первинного захисту інформаційних каналів для супутникових систем зв'язку. Баран, Ігор Олегович , грудень 2019 https://elartu.tntu.edu.ua/handle/lib/30606

6. Національний технічний університет України "Київський політехнічний інститут", 12.05.2015 https://studfile.net/preview/3740811/page:16/

7. Довженко, Н., Іваніченко, Є., & Костюк, Ю. (2025). Методика виявлення та локалізації кіберзагроз у хмарних середовищах з інтегрованими IoT-компонентами на основі графових моделей. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 762–776. https://doi.org/10.28925/2663-4023.2025.29.938

8. Методи та засоби захисту інформації: Конспект лекцій / Укладач В.І. Стаценко. Друге навчальне видання. Дніпро, ФТФ ДНУ, 2022 https://files.fti.dp.ua/wp-content/uploads/tainacan-items/2456/14592/metody-ta-zasoby-zakhystu-informatsii_.pdf

9. Хмарні сховища: що це та для чого вони потрібні https://gigacloud.ua/articles/hmarni-shovyshha-shho-cze-ta-dlya-chogo-vony-potribni/

10. Складанний, П., Машкіна, І., Рзаєва, С., & Костюк, Ю. (2025). Методи GDPR для забезпечення безпеки сховищ даних від витоків та загроз. Телекомунікаційні та інформаційні технології, 2(87), 59–76. https://doi.org/10.31673/2412-4338.2025.027860

11. Дослідження методів захисту у хмарних системах. Назаренко Д.М. Харківський Національний Університет Радіоелектроніки https://ice.nure.ua/wp-content/uploads/2024/01/50_Nazarenko-D.M.-_3_Str.170-172.pdf