Список використаних джерел:

1. Poesen, J., & Hooke, J. (1997). Erosion, flooding and channel management in Mediterranean environments. Progress in Physical Geography, 21(2), 157-199.
2. Kosmas, C., Gerontidis, S., & Marathianou, M. (2000). The effect of land use change on soil and vegetation over various lithological formations on Lesvos (Greece). Catena, 40(1), 51-68.
3. European Environment Agency (EEA). (2019). Soil conservation and sustainable land management in Greece.
4. Ministry of Environment and Energy of Greece. (2021). National Action Plan for Soil Protection.
5. FAO (Food and Agriculture Organization). (2020). Soil erosion assessment in the Mediterranean region.
6. United Nations Convention to Combat Desertification (UNCCD). (2022). Greece's strategies for soil protection and climate adaptation.

Abstract: *This paper examines the problem of soil erosion in Greece, its main causes, and negative consequences. Preventive and conservation measures aimed at preserving soil cover are analyzed, including agronomic methods, afforestation, engineering structures, and ecological farming. Special attention is given to measures for mitigating the effects of erosion and rehabilitating degraded lands. The role of legal regulation and state support in soil protection is also assessed.*
Keywords: *soil erosion, Greece, conservation measures, agronomy, afforestation, ecological farming, legal regulation, soil rehabilitation.*

Науковий керівник:
Шебаніна О.В.,
д-р екон. наук,
професор кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій ,
Миколаївський національний аграрний університет

УДК 004.056.55:004.438

Хешування як один із фундаментальних стовпів кібербезпеки

Владислав Макеєв,
здобувач вищої освіти спеціальності 122 Комп'ютерні науки
Миколаївський національний аграрний університет
м. Миколаїв, Україна

Анотація: *в сучасному цифровому світі, де обсяги інформації зростають експоненціально, а кібербезпека стає питанням першорядної важливості,*

технології хешування відіграють критичну роль. Хешування є фундаментальним інструментом криптографії, що використовується для забезпечення цілісності даних, захисту паролів, створення цифрових підписів та в багатьох інших аспектах кібербезпеки. Розуміння принципів роботи хешування, його можливостей та обмежень є необхідним для кожного фахівця в області інформаційних технологій та кібербезпеки.
Ключові слова: *хешування, алгоритм, кібербезпека, цілісність даних, криптографія, хеш-функція.*

Хешування – це процес, який перетворює дані довільної довжини у вихідний рядок фіксованої довжини, відомий як хеш, хеш-значення або дайджест. Це перетворення здійснюється за допомогою спеціальної математичної функції, яка називається хеш-функцією. Існує кілька основних принципів, які регулюють процес хешування.

Однією з ключових характеристик хеш-функції є її односпрямованість. Хеш-функцію можна легко обчислити в одному напрямку, від даних до хешу. Проте обернений процес – відновлення оригінальних даних з хешу – повинен бути обчислювально неможливим або надзвичайно складним. Ця властивість є важливою для безпеки, особливо при зберіганні паролів.

Ще одним важливим принципом є детермінованість. Для одних і тих же вхідних даних хеш-функція завжди повинна генерувати одне і те ж хеш-значення. Це гарантує стабільність і передбачуваність результатів, що дозволяє користувачам послідовно перевіряти цілісність даних.

Крім того, хеші, що виробляються хеш-функцією, мають фіксовану довжину, незалежно від розміру вхідних даних. Наприклад, хеш-функція SHA-256 завжди виробляє хеш довжиною 256 біт, чи ви хешуєте одне слово, чи цілу книгу. Ця характеристика забезпечує однорідність у виходах хешів, що є важливим для різних застосувань.

Нарешті, чутливість до змін є критично важливим аспектом хешування. Невелика зміна у вхідних даних повинна призводити до суттєвої зміни у хеш-значенні. Ця особливість є життєво важливою для підтримки цілісності даних, оскільки навіть маленька модифікація у файлі призведе до абсолютно іншого хешу, миттєво сигналізуючи про будь-які несанкціоновані зміни.

Хешування є потужним процесом, який використовується для захисту та перевірки даних завдяки своїм унікальним властивостям, які включають односпрямовану функціональність, детермінованість, фіксовану довжину виходу та чутливість до змін. Ці характеристики роблять хешування незамінним інструментом у різних сферах, особливо в кібербезпеці та перевірці цілісності даних.

Слід зазначити, що для використання в криптографії хеш-функції повинні бути достатньо стійкими і захищеними від зворотного процесу знаходження вихідних даних. Тут з’являється поняття колізії. Вона виникає коли два різних вхідних значення генеруються як одне й теж хеш-значення. Ідеальна криптографічна хеш-функція повинна мати надзвичайно низьку ймовірність

колізій. Хоча колізії теоретично існують (через принцип Діріхле, оскільки вхідних даних потенційно нескінченно багато, а вихід хешу обмежений), для надійних хеш-функцій пошук колізій повинен бути практично нездійсненним. Якщо колізії легко знайти, це може бути використано для атак, наприклад, для підробки цифрових підписів.

Одним з найважливіших застосувань хешування в кібербезпеці є захист паролів. Замість того, щоб зберігати паролі користувачів у чистому вигляді в базах даних, системи зберігають лише хеші цих паролів. Коли користувач намагається увійти в систему, введений ним пароль проходить процес хешування, і отриманий хеш порівнюється зі збереженим хешем. Якщо хеші збігаються, автентифікація вважається успішною.

Переваги цього підходу є значними. По-перше, він забезпечує захист від витоку даних. Навіть якщо база даних паролів буде скомпрометована, зловмисники отримають лише хеші, а не самі паролі. Завдяки властивості односпрямованості, відновлення паролів з хешів є обчислювально складним завданням, що додає ще один рівень безпеки. По-друге, даний метод зменшує ризик внутрішніх загроз. Адміністратори системи або інші особи з доступом до бази даних не можуть дізнатися паролі користувачів, оскільки зберігаються лише хеші. Це забезпечує конфіденційність і захист особистих даних користувачів, що є критично важливим у сучасному цифровому світі. Таким чином, хешування паролів є ключовим елементом у забезпеченні безпеки інформаційних систем, сприяючи захисту даних та зменшенню ризиків, пов'язаних з витоками інформації.

Хешування ефективно використовується для перевірки цілісності даних. Для файлу або набору даних обчислюється хеш-значення та зберігається окремо (наприклад, разом з файлом або в базі даних). Наприклад під час передачі файлів через мережу або їх зберігання на носіях, можуть виникати пошкодження. Порівняння хешів до та після передачі/зберігання дозволяє виявити такі пошкодження.

Серед переваг навіть для звичайного користувача є також перевірка оригінальності програмного забезпечення. Сайти розробників часто публікують хеш-суми для завантажуваних файлів програмного забезпечення. Користувачі можуть перевірити цілісність завантаженого файлу, обчисливши його хеш та порівнявши з опублікованим хешем. Це допомагає переконатися, що завантажений файл є оригінальним і не був модифікований зловмисниками. Така перевірка ще допомагає перевірити версію програми. Наприклад у системах контролю версій (наприклад, Git) хеші використовуються для ідентифікації версій файлів та для перевірки цілісності репозиторію.

Цифрові підписи та сертифікати є ключовими компонентами інфраструктури відкритого ключа (PKI) та використовуються для забезпечення автентичності та цілісності цифрових документів та комунікацій. Процес створення цифрового підпису зазвичай включає хешування документа, що підписується. Потім, хеш-значення підписується приватним ключем відправника. Таким чином зменшується розмір даних, а унікальна прив’язка

зберігається. Цифрові сертифікати використовуються для підтвердження автентичності відкритого ключа. Сертифікат містить відкритий ключ, ідентифікаційну інформацію власника ключа та підпис центру сертифікації (CA). Браузери та операційні системи використовують відкриті ключі CA, вбудовані в них, для перевірки цифрових сертифікатів сайтів та іншого програмного забезпечення.

Таким чином, хешування є одним із фундаментальних стовпів кібербезпеки, оскільки забезпечує цілісність та автентичність інформації. Хеш-функції, такі як SHA-256 чи MD5, широко використовуються для зберігання паролів, перевірки цілісності файлів та цифрового підпису. Основні властивості хешування роблять його критично важливим для захисту конфіденційної інформації.

Список використаних джерел:

1. GeeksforGeeks. Introduction to Hashing. GeeksforGeeks. URL: https://www.geeksforgeeks.org/introduction-to-hashing-2/?ref=header_outind.

2. blog.whitebit.com. Що таке хеш у блокчейні?
URL: https://blog.whitebit.com/uk/what-is-a-hash-in-blockchain/

3. What is SHA-2 and how does it work?. Comparitech.
URL:
https://www.comparitech.com/blog/information-security/what-is-sha-2-how-does-it-work/.

Abstract: *In today's digital world, where the volume of information is growing exponentially, and cybersecurity is becoming a matter of paramount importance, hashing technologies play a critical role. Hashing is a fundamental cryptography tool used to ensure data integrity, password protection, digital signature creation and many other aspects of cybersecurity. Understanding the principles of hashing, its capabilities and limitations is necessary for every specialist in areas of information technology and cybersecurity.*

Keywords: *Hashing, algorithm, cybersecurity, data integrity, cryptography, hash function.*

Науковий керівник:
Пархоменко О. Ю.,
к. ф.-м. н., доцент кафедри економічної кібернетики,
комп'ютерних наук та інформаційних технологій,
Миколаївський національний аграрний університет