

ПРО МЕТОДИ КОНТРОЛЮ ЦІЛІСНОСТІ ДАНИХ

Вінницький національний технічний університет

Анотація В цих тезах розглянуто сучасні методи забезпечення контролю цілісності даних в інформаційних системах. Аналізуються традиційні криптографічні методи (хеш-функції, коди автентифікації повідомлень – MAC, електронний цифровий підпис – ЕЦП) та сучасні підходи (алгоритми на основі універсальних кодів автентифікації повідомлень – UMAC).

Ключеві слова: цілісність даних, хеш-функція, код автентифікації повідомлень (MAC), універсальний код автентифікації повідомлень (UMAC), криптографія, цифровий підпис, кібербезпека.

Abstract. In these theses, modern methods of ensuring data integrity control in information systems are considered. Traditional cryptographic methods (hash functions, message authentication codes – MAC, electronic digital signature – EDS) and modern approaches (algorithms based on universal message authentication codes – UMAC) are analyzed.

Keywords: data integrity, hash function, message authentication code (MAC), universal message authentication code (UMAC), cryptography, digital signature, cybersecurity.

Вступ

У великих корпораціях забезпечення контролю цілісності даних є критично важливим аспектом безпеки інформаційних систем, що запобігає несанкціонованим змінам або спотворенню даних. Для цього використовуються різноманітні методи та технології, охоплюючи і математичні, і криптографічні підходи, що дозволяють гарантувати достовірність інформації протягом всього її життєвого циклу – від первинного введення до зберігання чи остаточного використання.

Вимоги чинного законодавства України, ДСТУ ISO/IEC 27001:2023 “Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги”, ДСТУ ISO/IEC 27002:2023 “Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки” диктують використання широкого спектру методів контролю цілісності даних. Використання таких стандартів сприяє ефективній інтеграції методів контролю цілісності даних у сучасні інформаційні системи.

Сучасні методи контролю цілісності даних враховують специфіку різних сфер застосування, зокрема банківських систем, де забезпечення достовірності даних є вирішальним для безпеки транзакцій. Наприклад, у автоматизованих банк-системах використання цифрових підписів та методів перевірки цілісності забезпечує надійний захист від атак типу «людина посередині» (man-in-the-middle), що є найбільш розповсюдженими загрозами у фінансових операціях [1].

Метою дослідження є огляд відомих методів контролю цілісності даних.

Результати дослідження

Одним із основних методів забезпечення цілісності даних є використання хеш-функцій. Хешування перетворює повідомлення довільної довжини у фіксований розмір, що значно спрощує процес перевірки цілісності даних. Як помічено в [2], застосування хеш-функцій у криптографії забезпечує високу стійкість до модифікацій та несанкціонованого доступу. Крім того, хешування може бути інтегроване в різноманітні системи автентифікації та схеми цифрових підписів, що додає додатковий рівень захисту.

Проте хеш-функції не є єдиним засобом забезпечення цілісності даних. У більш складних системах застосовуються криптографічні коди автентифікації повідомлень (MAC), що дозволяють не лише перевірити цілісність інформації, але й автентифікувати відправника. Це особливо важливо, коли дані передаються через незахищені канали зв'язку. Як підкреслюють в [3], використання криптографічних кодів є ефективним засобом захисту фінансових та банківських систем від атак, спрямованих на підробку або зміну даних.

На додаток до стандартних методів хешування та MAC, сьогодні активно впроваджуються нові підходи, зокрема алгоритми на основі універсальних кодів автентифікації повідомлень (UMAC). Такі

алгоритми забезпечують високу швидкість перевірки з мінімальними обчислювальними витратами, гарантують стійкість до колізій і ефективно протидіють різноманітним атакам [4].

До методів контролю цілісності даних належать:

1) Повна копія даних. Створюються повні копії даних, а потім порівнюються з оригіналом. Дозволяє виявити будь-які зміни та відновити дані у разі порушення цілісності. Перевагою є простота реалізації та повний контроль над даними, а недоліками є великий обсяг копії, а також можливість підробки та крадіжки копії.

2) Контрольна сума. Наприклад, CRC. За вхідними даними з допомогою певного алгоритму розраховується значення. Перевагами є висока швидкість обчислення та невеликий розмір. Недоліками є те, що для одного значення існує безліч вихідних даних, є можливість підібрати вихідні дані до значення.

3) Хеш. Використання криптографічних алгоритмів для розрахунку унікального значення за вхідними даними. Перевагами є малий розмір та неможливість підбору вихідних даних до значення. З недоліків можна назвати низьку швидкість обчислення.

4) Імітовставка (MAC). Значення, розраховане за вхідними даними з використанням ключа, відомого лише відправнику та одержувачу. Перевагами є невеликий розмір, вибір вихідних даних до значення без ключа та підміна без ключа неможливі. Недоліками є низька швидкість обчислення, існування множини вихідних даних для одного значення, а також можливість крадіжки ключа.

5) Електронний цифровий підпис (ЕЦП). Унікальний підпис даних на основі хеш-функцій та асиметричного шифрування (RSA, ECDSA, EdDSA) для підтвердження ідентичності користувача та підтвердження цілісності даних. Перевагами є мінімальний розмір, неможливість підбору вихідних даних до значення без ключа. Недоліками є низька швидкість обчислення.

Ці методи дозволяють захищати дані від несанкціонованих змін та гарантувати їхню достовірність протягом всього життєвого циклу. Особлива увага приділена застосуванню даних технологій у критичних секторах, де забезпечення цілісності даних є надзвичайно важливим для підтримки високого рівня безпеки та довіри. Дослідження також враховує відповідність існуючим криптографічним стандартам, що сприяє ефективній інтеграції методів захисту інформації в сучасні інформаційні технології. Комплексний аналіз теоретичних концепцій і практичних застосувань демонструє, що надійний контроль цілісності даних є ключовим інструментом для протидії сучасним кіберзагрозам та забезпечення загальної кібербезпеки.

Висновки

Загалом, методи контролю цілісності даних є невід'ємною складовою інформаційної безпеки. Їх постійне вдосконалення та адаптація до нових технологій є ключовими для протидії сучасним кіберзагрозам. Вибір оптимального методу залежить від специфіки застосування, обсягу оброблюваних даних та вимог до безпеки системи. Добре продумана стратегія контролю цілісності даних не лише підвищує рівень захисту конфіденційної інформації, а й зміцнює довіру до цифрових комунікацій та транзакцій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Hryshchuk R., Yevseiev S., Shmatko A. Construction methodology of information security system of banking information in automated banking systems // Monograph", Premier Publishing s. r. o. – Vienna. – 2018. – Pp. 134-156.
2. Євсєєв С.П., Йохов О.Ю., Король О.Г. Гешування даних в інформаційних системах // Монографія Харків: Вид. ХНЕУ. – 2013. – 312 с.
3. Євсєєв С. П., Король О.Г., Жукарев В.Ю. Технології комп'ютерних мереж. // Мультимедійне інтерактивне електронне видання комбінованого використання. – Х.: ХНЕУ ім. С. Кузнеця. – 2015. – 207с.
4. Korol Olha, Havrylova Alla, Yevseiev Serhii Practical UMAC algorithms based on crypto code designs // Przetwarzanie, transmisja i bezpieczeństwo informacji, Bielsko-Biala: Wydawnictwo naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej. –2019. – Tom 2. – Pp. 221-232.

Крайнічук (Шелепало) Галина Василівна – к. фіз.-мат. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна, email: hv.shelepalo@vntu.edu.ua

Долінський Ростислав Олегович – студент групи ІБК-216, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, email: rdolinskij49@gmail.com

Krainichuk (Shelepalo) Halyna – PhD (eng), associated professor of information protection department, Vinnytsia National Technical University, Vinnytsia, email: hv.shelepalo@vntu.edu.ua

Rostislav Dolinsky – student of ІБК-216 group, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine, email: rdolinskij49@gmail.com