УДК 004.056:004.738.5

А. В. Чеснов
О. В. Салієва

ПІДВИЩЕНЯ РІВНЯ БЕЗПЕКИ ЛОКАЛЬНОГО СХОВИЩА ДАНИХ ВЕБДОДАТКІВ ШЛЯХОМ СЕГМЕНТАЦІЇ ДАНИХ ТА КРИПТОГРАФІЧНОЇ ІДЕНТИФІКАЦІЇ ПРИСТРОЮ

Вінницький національний технічний університет

Анотація

У роботі розглядається підхід до підвищення рівня безпеки локального сховища даних вебдодатків шляхом використання сегментації даних та криптографічної ідентифікації пристрою користувача. Запропоновано механізм розподілу конфіденційної інформації на окремі сегменти з їх подальшим зберіганням у різних структурах браузерного середовища, що ускладнює несанкціонований доступ до цілісних даних. Для забезпечення додаткового рівня захисту використано криптографічну прив'язку ключів шифрування до параметрів пристрою та браузера користувача, що дозволяє мінімізувати ризики компрометації даних при викраденні токенів або локальних файлів сховища. Досліджено основні вразливості локальних сховищ вебдодатків та обґрунтовано доцільність застосування динамічного шифрування й адаптивної генерації криптографічних ключів. Реалізація запропонованого підходу спрямована на підвищення конфіденційності, цілісності та стійкості даних до сучасних кіберзагроз.

Ключові слова: вебдодатки, Local Storage, захист даних, сегментація даних, криптографічна ідентифікація, динамічне шифрування, інформаційна безпека, браузер, конфіденційні дані.

Abstract

The paper considers an approach to increasing the security level of local data storage of web applications by using data segmentation and cryptographic identification of the user's device. A mechanism is proposed for dividing confidential information into separate segments with their subsequent storage in different stuctures of the browser environment, which makes unauthorized access to integral data more difficult. To provide an additional level of protection, cryptographic binding of encryption keys to the parameters of the user's device and browser is used, which allows minimizing the risks of data compromise when stealing tokens or local files of the storage. The main vulnerabilities of local web application repositories are investigated and the feasibility of using dynamic encryption and adaptive cryptographic key generation is substantiated. The implementation of the proposed approach is aimed at increasing the confidentiality, integrity and resilience of data to modern cyber threats.

Keywords: web applications, Local storage, data protection, data segmentation, cryptographic identification, dynamic encryption, information security, browser, confidential data.

Вступ

Стрімкий розвиток вебтехнологій та зростання кількості вебдодатків призводять до активного використання локальних сховищ браузера для зберігання користувацьких даних, токенів автентифікації та параметрів сесії. Використання таких механізмів, як Local Storage та Session Storage, дозволяє підвищити продуктивність вебдодатків і забезпечити швидкий доступ до інформації без постійного звернення до сервера. Однак зберігання конфіденційних даних у локальному середовищі браузера супроводжується значними ризиками, пов'язаними з несанкціонованим доступом, XSS-атаками, викраденням токенів та компрометацією користувацьких даних.

Одним із перспективних напрямів підвищення рівня безпеки локального сховища є використання методів сегментації даних та криптографічного захисту. Сегментація дозволяє розподіляти інформацію на окремі логічні частини, що ускладнює отримання цілісних даних зловмисником навіть у випадку часткового доступу до сховища. Додатковий рівень захисту забезпечується шляхом застосування криптографічної ідентифікації пристрою, за якої ключі шифрування формуються з урахуванням параметрів браузера та апаратного середовища користувача. Такий підхід значно знижує ймовірність використання викрадених даних на сторонніх пристроях.

У роботі досліджується можливість підвищення рівня безпеки локального сховища даних вебдодатків шляхом поєднання сегментації інформації, динамічного шифрування та криптографічної прив'язки до параметрів пристрою користувача. Запропонований підхід спрямований на забезпечення конфіденційності та цілісності даних, а також підвищення стійкості вебдодатків до сучасних кіберзагроз. Практична реалізація такого механізму може бути використана у вебсистемах, що працюють із персональними або критично важливими даними та потребують підвищеного рівня інформаційної безпеки.

Результати досліджень

Основною проблемою сучасних вебдодатків є забезпечення безпечного зберігання конфіденційних даних у клієнтському середовищі. Більшість сучасних вебсистем використовують Local Storage, Session Storage або IndexedDB для зберігання токенів автентифікації, параметрів користувацьких сесій, налаштувань інтерфейсу та службових даних. Використання локальних сховищ забезпечує високу швидкість доступу до інформації та зменшує навантаження на серверну частину системи, однак одночасно створює значні ризики інформаційної безпеки. Основними загрозами є XSS-атаки, викрадення JWT-токенів, підміна локальних даних, компрометація браузерного середовища та несанкціонований доступ до конфіденційної інформації через шкідливі скрипти [1].

Традиційні механізми захисту, що базуються лише на HTTPS, HttpOnly-cookie або стандартних алгоритмах шифрування, не забезпечують достатнього рівня безпеки у випадку компрометації браузерного середовища користувача. У більшості випадків дані у Local Storage зберігаються у відкритому вигляді або з використанням статичних ключів шифрування, що значно спрощує їх викрадення та повторне використання. Особливо небезпечними є сценарії, у яких зловмисник отримує копію локального сховища або токенів авторизації та використовує їх на іншому пристрої без додаткової перевірки середовища виконання [2]. У зв'язку з цим актуальним є створення механізмів захисту, які б забезпечували не лише шифрування даних, але й їх криптографічну прив'язку до конкретного пристрою та браузерного середовища.

Для підвищення рівня безпеки локального сховища у роботі запропоновано використання комбінованого підходу, що поєднує сегментацію даних, динамічне шифрування та криптографічну ідентифікацію пристрою користувача. Сегментація даних передбачає розподіл конфіденційної інформації на окремі незалежні логічні частини. Наприклад, токен авторизації може бути поділений на декілька сегментів, що зберігаються у різних структурах браузерного середовища: частина у Local Storage, частина у Session Storage, а окремі службові параметри — у пам'яті активної сесії. Такий підхід значно ускладнює отримання повного набору даних навіть у випадку часткового компрометування локального середовища [3].

Додатковим рівнем захисту виступає динамічне шифрування сегментів даних. На відміну від традиційного підходу із використанням статичних ключів, запропонована система формує криптографічний ключ на основі параметрів конкретного пристрою користувача. Для генерації ключа можуть використовуватися User-Agent браузера, тип операційної системи, часові параметри сесії, характеристики дисплея, мова браузера, параметри апаратного середовища та інші ідентифікаційні ознаки. У результаті навіть при викраденні локальних даних або сегментів токенів їх використання на іншому пристрої стає неможливим через невідповідність параметрів генерації криптографічного ключа [4].

Важливим елементом запропонованої системи є механізм ротації криптографічних ключів та автоматичного оновлення сегментів сховища після кожної успішної сесії автентифікації. Після завершення користувацької сесії система формує новий ключ шифрування та повторно шифрує сегменти даних із використанням оновлених параметрів середовища. Це дозволяє значно знизити ризик повторного використання викрадених токенів або локальних файлів браузера. Крім того, реалізація часових обмежень доступу до сегментів даних забезпечує додатковий рівень контролю над безпечністю зберігання інформації [5].

Запропонований підхід також дозволяє зменшити наслідки XSS-атак. У традиційних вебдодатках шкідливий скрипт може отримати повний доступ до Local Storage та викрасти всі токени автентифікації. У випадку сегментованого сховища з динамічним шифруванням зловмисник отримує лише окремі зашифровані частини даних, які неможливо використати без параметрів пристрою та

алгоритму формування ключа. Таким чином, навіть у випадку часткового витоку інформації рівень ризику суттєво знижується.

Практична реалізація запропонованого механізму може бути виконана із використанням сучасних криптографічних бібліотек Web Crypto API, що забезпечують підтримку алгоритмів AES-GCM, SHA-256 та PBKDF2 для генерації ключів шифрування [6]. Використання Web Crypto API дозволяє реалізувати криптографічні операції безпосередньо у браузері користувача без необхідності передачі ключів на серверну сторону. Це підвищує рівень конфіденційності даних та зменшує ризик компрометації централізованого сховища ключів.

У результаті проведеного дослідження встановлено, що традиційні методи зберігання даних у Local Storage та Session Storage не забезпечують достатнього рівня захисту конфіденційної інформації у вебдодатках. Аналіз основних вразливостей браузерного середовища показав, що зловмисники можуть отримувати доступ до токенів автентифікації, параметрів сесії та інших критично важливих даних через XSS-атаки, викрадення локальних файлів браузера або компрометацію клієнтського середовища. Визначено, що використання статичних ключів шифрування та централізованого зберігання інформації значно підвищує ризик повторного використання викрадених даних.

У ході дослідження розроблено модель сегментації конфіденційної інформації, відповідно до якої дані поділяються на окремі логічні сегменти та зберігаються у різних структурах браузерного середовища. Такий підхід дозволяє мінімізувати ризик отримання повного набору даних навіть у випадку часткової компрометації локального сховища. Встановлено, що сегментоване зберігання значно ускладнює автоматизоване викрадення токенів та службової інформації шкідливими скриптами.

Також запропоновано механізм динамічного шифрування даних із використанням криптографічної прив’язки до параметрів пристрою та браузера користувача. У процесі дослідження визначено, що використання таких параметрів, як User-Agent, тип операційної системи, часові характеристики сесії та конфігурація браузера, дозволяє формувати унікальні криптографічні ключі для кожного користувацького середовища. Це забезпечує неможливість коректного розшифрування даних на сторонньому пристрої навіть у випадку фізичного копіювання локального сховища або викрадення токенів автентифікації.

Результати дослідження показали, що використання механізму ротації криптографічних ключів після кожної успішної сесії автентифікації підвищує стійкість системи до атак повторного використання сесій. Крім того, реалізація адаптивного оновлення сегментів даних дозволяє знизити ризик довготривалого використання компрометованих токенів. Проведений аналіз підтвердив, що поєднання сегментації даних, динамічного шифрування та криптографічної ідентифікації пристрою суттєво підвищує рівень конфіденційності, цілісності та захищеності локального сховища вебдодатків.

Отримані результати можуть бути використані під час розробки сучасних вебсистем, що працюють із персональними, фінансовими або критично важливими даними та потребують підвищеного рівня інформаційної безпеки. Запропонований підхід створює основу для подальшого розвитку механізмів захисту клієнтського середовища вебдодатків із використанням адаптивних криптографічних технологій та поведінкового аналізу користувача.

Висновки

У роботі було досліджено підхід до підвищення рівня безпеки локального сховища даних вебдодатків, що ґрунтується на поєднанні сегментації даних та криптографічної прив’язки до параметрів пристрою користувача. Встановлено, що традиційні механізми зберігання інформації у браузерному середовищі, зокрема Local Storage та Session Storage, мають суттєві обмеження щодо захисту від несанкціонованого доступу, що зумовлює необхідність застосування додаткових рівнів безпеки.

Запропонований механізм сегментації конфіденційних даних дозволяє розподіляти інформацію на окремі частини з їх подальшим зберіганням у різних структурах браузерного середовища. Такий підхід значно ускладнює відновлення цілісного набору даних у разі компрометації окремих елементів сховища, тим самим підвищуючи загальний рівень захищеності вебдодатку.

Додатково обґрунтовано ефективність використання криптографічної прив’язки ключів шифрування до унікальних характеристик пристрою та браузера користувача. Це дозволяє

мінімізувати ризики використання викрадених токенів або локальних файлів сховища на сторонніх пристроях, оскільки доступ до даних стає можливим лише в межах довіреного середовища.

У результаті дослідження доведено, що поєднання динамічного шифрування, сегментації даних та адаптивної генерації криптографічних ключів є ефективним напрямом підвищення безпеки локального зберігання даних у вебдодатках. Запропонований підхід забезпечує підвищення конфіденційності, цілісності та стійкості інформації до сучасних кіберзагроз і може бути використаний у практичних вебрішеннях з підвищеними вимогами до захисту даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. HTML5 Security Cheat Sheet URL **:** https://cheatsheetseries.owasp.org/cheatsheets/HTML5_Security_Cheat_Sheet.html (дата звернення: 18.05.2026)
2. Cross Site Scripting Prevention Cheat Sheet URL: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html (дата звернення: 18.05.2026)
3. Mozilla Developer Network (MDN). Web Storage API.URL: https://developer.mozilla.org/enUS/docs/Web/API/Web_Storage_API (дата звернення: 18.05.2026)
4. Stallings W. Cryptography and Network Security: Principles and Practice Authentication URL: https://www.pearson.com/en-us/subject-catalog/p/cryptography-and-network-security-principles-and-practice/P200000003477/9780135764213?srsltid=AfmBOorC_D3kRsaAnzGq8SQ0dwd8L3ciilI1eMAJO0qUgWykdwDWSYZi (дата звернення: 18.05.2026)
5. Ferguson N., Schneier B., Kohno T. Cryptography Engineering URL: https://www.researchgate.net/publication/220691667_Cryptography_Engineering_Design_Principles_and_Practical_Applications (дата звернення: 18.05.2026)
6. Mozilla Developer Network (MDN). Web Crypto API. URL: https://developer.mozilla.org/en US/docs/Web/API/Web_Crypto_API (дата звернення: 18.05.2026)

Чеснов Артем В'ячеславович – студент групи 1КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: chesnovatremon@gmail.com

Науковий керівник: ***Салієва Ольга Володимирівна*** – доктор філософії (PhD) за спеціальністю 125 "Кібербезпека", доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@vntu.edu.ua

Chesnov Artem V. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: chesnovatremon@gmail.com

Supervisor*:* ***Saliieva Olha V.*** – Doctor of Philosophy (PhD) in specialty 125 "Cybersecurity", Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, email: salieva8257@ vntu.edu.ua