УДК 004.056.5 Научная статья
DOI: 10.35330/1991-6639-2024-26-1-39-47
EDN: GEVSAQ

Разработка подхода к обеспечению информационной безопасности в веб-ориентированных информационных системах при передаче данных с использованием интерфейса Web Cryptography API

М. В. Ступина

Донской государственный технический университет
344003, Россия, ЮФО, г. Ростов-на-Дону, пл. Гагарина, 1

Аннотация. Целью исследования является формулирование общих принципов обеспечения информационной безопасности в веб-ориентированных информационных системах. В работе описаны основные концепции интерфейса Web Cryptography API, а также представлены практические аспекты использования криптографических методов для обеспечения безопасности данных веб-ориентированных информационных систем. Предложенный подход, основанный на введении безопасной системы генерации и хранения приватных ключей пользователей через использование асинхронного алгоритма шифрования ECDSA средствами интерфейса Web Cryptography API, в сочетании с шифрованием приватных ключей кодовыми словами и дополнительной аутентификацией пользователей позволяет обеспечить высокий уровень защиты приватных ключей от несанкционированного доступа.

Ключевые слова*:* Web Cryptography API, криптография, электронная подпись, электронный документооборот, ECDSA

СПИСОК ЛИТЕРАТУРЫ

1. *Мехдиев Э. Т., Плеханова Е. А.* Развитие систем электронного документооборота в цифровой экономике // Дискуссия. 2023. № 1(116). С. 58–70. DOI: 10.46320/2077-7639-2022-6-115-52-70

2. *Гончаров Е. И., Шатковская Т. В.* Проблемы применения цифровой подписи в электронном документообороте России // Северо-Кавказский юридический вестник. 2020. № 2. С. 97–103. DOI: 10.22394/2074-7306-2020-1-2-97-103

3. *Баранов А. С.* Использование средств криптографической защиты информации в организациях // Международный научно-исследовательский журнал. 2020. № 6-1 (96). С. 131–133. DOI: 10.23670/IRJ.2020.96.6.023

4. *Былинский М. Д.* Защита приложений javascript с помощью Web Cryptography Api // Вестник Балтийского федерального университета им. И. Канта. Серия: Физико-математические и технические науки. 2022. № 1. С. 53–60.

5. *Cairns K., Halpin H., Steel G.* Security Analysis of the W3C Web Cryptography API // Proceedings of Security Standardisation Research (SSR). Gaithersberg. 2017. Pp. 112–140. DOI: 10.1007/978-3-319-49100-4_5

6. *Wichmann P., Blochberger M., Federrath H.* Web Cryptography API // Prevalence and Possible Developer Mistakes. In Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22). Association for Computing Machinery. New York. 2022. Pp. 1–10. DOI: 10.1145/3538969.3538977

7. *Samir A., Abo-Taleb M., Shalaby, Nabil M., Elramly S.* A Side-Channel Attack Resistive ECDSA // International Conference on Advanced Information Systems and Engineering. Journal of Physics: Conference Series. Cairo, Egypt. 2019. Pp. 112–140. DOI: 10.1088/1742-6596/1454/1/012003

Информация об авторе

Ступина Мария Валерьевна, канд. пед. наук, доцент кафедры информационных технологий, Донской государственный технический университет;

344003, Россия, г. Ростов-на-Дону, пл. Гагарина, 1;

masamvs@bk.ru, ORCID: https://orcid.org/0000-0002-6394-6966