РЕФЕРАТ

Актуальність теми. Магістерська дисертація присвячена розробці та аналізу модифікованого алгоритму Time-Based One-Time Password для обмеження доступу до ресурсів у високонавантажених системах, важлива у сфері кібербезпеки та технологій. У сучасному цифровому середовищі, захист інформації від кіберзагроз є надзвичайно актуальним. Високонавантажені системи потребують ефективного та швидкого методу автентифікації, щоб забезпечити безпеку та уникнути перевантаження ресурсів. Модифікований алгоритм TOTP може стати ефективним інструментом для забезпечення безпеки та зниження навантаження на систему. Таке дослідження має велике значення для поліпшення методів захисту та забезпечення стійкості та швидкості доступу у високонавантажених системах

Об'єктом дослідження є використання алгоритму Time-Based One-Time Password (TOTP) для обмеження доступу до ресурсів у високонавантажених системах.

Предметом дослідження є розробка та аналіз модифікованого алгоритму Time-Based One-Time Password (TOTP) для оптимізації та підвищення безпеки обмеження доступу до ресурсів у високонавантажених системах.

Мета роботи: полягає у вивченні, розробці та оцінці модифікованого алгоритму Time-Based One-Time Password (TOTP) для підвищення ефективності та безпеки обмеження доступу до ресурсів у високонавантажених системах. Основними цілями є аналіз існуючих методів обмеження доступу, розробка модифікованого алгоритму TOTP, виявлення та оцінка його переваг у контексті ефективності, надійності та стійкості до потенційних кіберзагроз. Мета також включає в себе визначення оптимальних умов та сценаріїв застосування цього алгоритму в високонавантажених системах, забезпечуючи високу захищеність та зниження негативного впливу на продуктивність системи.

Наукова новизна цієї роботи полягає у розробці та аналізі модифікованого алгоритму TOTP з метою покращення процесу обмеження доступу до ресурсів у високонавантажених системах. Цей алгоритм включає в себе нові методи генерації та верифікації одноразових паролів на основі часу, що сприяє підвищенню ефективності, стійкості та безпеки систем у порівнянні зі стандартними методами аутентифікації. Дослідження також враховує оптимізацію алгоритму для роботи у високонавантажених середовищах, що відрізняється від попередніх підходів та є актуальною новизною у сфері кібербезпеки та застосування алгоритмів аутентифікації в сучасних інформаційних системах.

Практична цінність отримані результати дослідження мають велику практичну цінність у сферах бізнесу, фінансів, електронної комерції та інших сферах. Вони можуть служити основою для покращення інформаційної безпеки через розробку та впровадження більш надійних систем захисту даних та методів автентифікації.

Апробація роботи. Основні положення були представлені та обговорювались на CXXXIV Міжнародній інтернет-конференції «Сучасні аспекти розвитку науки і техніки в умовах війни» та LVVI Міжнародної інтернет-конференції «Наука 2023: Дослідження та інновації»

Структура та обсяг роботи. Магістерська дисертація складається з вступу, чотирьох розділів та висновків.

У *вступі* проведено огляд загальної характеристики роботи, яка зорієнтована на важливі аспекти інформаційної безпеки та наявні методи захисту інформації.

Перший розділ дослідження присвячено аналізу ключових аспектів кібербезпеки та ролі паролів у захисті особистих даних. Аналізуючи ці аспекти, було виявлено потенціал у токенах, заснованих на часі, як ефективному інструменті забезпечення тимчасової та унікальної ідентифікації.

У другому розділі проведено аналіз різноманітних методів створення одноразових паролів, виокремлено їх переваги та недоліки. Одноразові паролі виступають важливим інструментом у захисті даних, а вибір конкретного методу генерації залежить від контексту та вимог безпеки системи.

Розділ третій складається з дослідження та аналізу різних методів імплементації алгоритму обмеження доступу до ресурсів за часовим параметром. Основна увага приділена модифікації токена Time-Based One-Time Password (TOTP) та обґрунтуванню вибору конкретних інструментів та методів для його модифікації.

Четвертий розділ містить результати тестування модифікованого алгоритму та показав його високу швидкодію, ефективність у використанні ресурсів та стійкість до атак.

У *висновках* представлені результати проведеної роботи.

Робота представлена на 103 аркушах, містить посилання на список використаних літературних джерел.

Ключові слова: одноразові паролі, кібербезпека, автентифікація, захист інформації, криптографія, генерація паролів, розповсюдження паролів, TOTP.

ABSTRACT

Actuality of theme. The master's dissertation is dedicated to the development and analysis of the modified Time-Based One-Time Password algorithm for restricting access to resources in high-load systems, significant in the realm of cybersecurity and technology. In the modern digital environment, safeguarding information against cyber threats is exceedingly relevant. High-load systems require an efficient and rapid authentication method to ensure security and avoid resource overload. The modified TOTP algorithm could become an effective tool for ensuring security and reducing system load. Such research holds great significance in enhancing protection methods and ensuring the resilience and speed of access in high-load systems.

The object of the study is the use of the Time-Based One-Time Password (TOTP) algorithm for restricting access to resources in high-load systems.

The subject of the research is the development and analysis of the modified Time-Based One-Time Password (TOTP) algorithm to optimize and enhance security in restricting access to resources in high-load systems.

The purpose of the work: is to study, develop, and evaluate the modified Time-Based One-Time Password (TOTP) algorithm to enhance the efficiency and security of access restriction to resources in high-load systems. The main goals include analyzing existing access restriction methods, developing the modified TOTP algorithm, identifying and assessing its advantages concerning efficiency, reliability, and resilience against potential cyber threats. Additionally, the aim involves defining optimal conditions and scenarios for implementing this algorithm in high-load systems to ensure high security levels and mitigate negative impacts on system productivity.

The scientific novelty is the purpose of this work is to develop and analyze a modified TOTP algorithm aimed at improving the process of restricting access to resources in high-load systems. This algorithm incorporates novel methods for generating and verifying one-time passwords based on time, contributing to increased efficiency, resilience, and security of systems compared to standard

authentication methods. The research also considers optimizing the algorithm to operate in high-load environments, which distinguishes it from previous approaches and presents significant novelty in the field of cybersecurity and the application of authentication algorithms in modern information systems.

The practical value is the obtained research outcomes hold significant practical value across various domains such as business, finance, e-commerce, and others. They can serve as the foundation for enhancing information security by developing and implementing more reliable data protection systems and authentication methods.

Approbation of work. The main findings and ideas were presented and discussed at the CXXXIV International Internet Conference "Current Aspects of Science and Technology Development in Times of War" and the LVVI International Internet Conference "Science 2023: Research and Innovation".

Structure and scope of work. The master's thesis comprises an introduction, four chapters, and conclusions.

The *introduction* provides an overview of the general characteristics of the work, focusing on crucial aspects of information security and existing methods of information protection.

The first chapter delves into analyzing key aspects of cybersecurity and the role of passwords in safeguarding personal data. Through this analysis, the potential of time-based tokens as an effective tool for temporary and unique identification was identified.

The second chapter involves an analysis of various methods for generating one-time passwords, highlighting their advantages and disadvantages. One-time passwords play a significant role in data protection, and the selection of a specific generation method depends on the context and security requirements of the system.

The third chapter comprises the exploration and analysis of different methods for implementing access restriction algorithms based on time parameters. It focuses primarily on the modification of the Time-Based One-Time Password (TOTP) token and justifies the selection of specific tools and methods for its modification.

The fourth chapter presents the results of testing the modified algorithm, demonstrating its high speed, efficiency in resource utilization, and resistance to attacks.

The *conclusions* section encapsulates the findings of the conducted research. The thesis consists of 103 pages and includes a reference list of utilized literary sources.

Keywords: one-time passwords, cybersecurity, authentication, information security, cryptography, password generation, password distribution, TOTP.