MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Electronică și Telecomunicații
Departamentul Telecomunicații și Sistemele Electronice

Admis la susţinere

Şefă departament:

Tîrșu Valentina, conf. univ., dr.

_____

„____”_____ 2024

Анализ методов шифрования и защиты баз данных в веб-приложениях

Teza de master

Student: **Pavlovschi Ian**
grupa MMRT-221M

Conducător: **Tîrșu Valentina**
conf. univ., dr.

Chișinău, 2024

АННОТАЦИЯ

Тема: Анализ методов шифрования и защиты баз данных в веб-приложениях

Структура работы: Работа состоит из 71 страниц, включая введение, три основных раздела - теоретический, аналитический и проектный, заключение и библиографию.

Ключевые слова: шифрование, защита баз данных, веб-приложения, информационная безопасность, системы безопасности, кибербезопасность.

Область исследований: методы шифрования, защита информации в веб-приложениях, обеспечение безопасности данных в интернете.

Цель работы: Разработка и анализ методов шифрования и защиты данных в базах данных, используемых в веб-приложениях, с целью обеспечения их надежной защиты от несанкционированного доступа и других видов киберугроз.

Цели:

1. Изучить и проанализировать существующие методы шифрования и защиты данных.
2. Разработать эффективную систему защиты на базе современных технологий.
3. Выбрать и адаптировать оптимальные инструменты и решения для защиты данных.
4. Разработать стратегии управления и контроля за системой безопасности.
5. Провести анализ и оценку эффективности разработанной системы.

Применяемые методы: Исследование методов криптографической защиты, анализ систем безопасности данных, разработка и тестирование системы защиты.

Полученные результаты:

В ходе работы была разработана комплексная система защиты данных для веб-приложений, включающая современные методы шифрования и защиты. Были выбраны и успешно интегрированы инструменты и решения, позволяющие эффективно контролировать безопасность данных и предотвращать несанкционированный доступ. Результаты анализа показали повышение уровня безопасности и надежности системы, что подтверждает эффективность выбранных методов и подходов.

ADNOTARE

Tema: Analiza metodelor de criptare și de securitate a bazelor de date în aplicațiile Web

Structura lucrării: Lucrarea constă în 71 de pagini, incluzând introducerea, trei secțiuni principale - teoretică, analitică și de proiect, concluzia și bibliografia.

Cuvinte cheie: criptare, protecția bazelor de date, aplicații web, securitatea informației, sisteme de securitate, cibernetica.

Domeniul cercetării: metode de criptare, protejarea informațiilor în aplicațiile web, asigurarea securității datelor pe internet.

Scopul lucrării: Dezvoltarea și analizarea metodelor de criptare și protecție a datelor în bazele de date utilizate în aplicațiile web, în scopul asigurării unei protecții fiabile împotriva accesului neautorizat și altor tipuri de amenințări cibernetice.

Obiective:

1. Studierea și analizarea metodelor existente de criptare și protecție a datelor.
2. Dezvoltarea unui sistem eficient de protecție bazat pe tehnologii moderne.
3. Selectarea și adaptarea instrumentelor și soluțiilor optime pentru protecția datelor.
4. Dezvoltarea de strategii pentru gestionarea și controlul sistemului de securitate.
5. Realizarea unei analize și evaluări a eficacității sistemului dezvoltat.

Metode utilizate: Cercetarea metodelor de protecție criptografică, analiza sistemelor de securitate a datelor, dezvoltarea și testarea sistemului de protecție.

Rezultate obținute:

În cadrul lucrării a fost dezvoltat un sistem complex de protecție a datelor pentru aplicațiile web, care include metode moderne de criptare și protecție. Au fost selectate și integrate cu succes instrumente și soluții care permit controlul eficient al securității datelor și prevenirea accesului neautorizat. Rezultatele analizei au arătat o creștere a nivelului de securitate și fiabilitate a sistemului, confirmând eficacitatea metodelor și abordărilor alese.

ANNOTATION

Topic: Analyzing encryption and database security methods in web applications

Work Structure: The work consists of 71 pages, including an introduction, three main sections - theoretical, analytical, and project, conclusion, and bibliography.

Keywords: encryption, database protection, web applications, information security, security systems, cybersecurity.

Research Area: encryption methods, data protection in web applications, ensuring data security on the internet.

Work Objective: Development and analysis of encryption and data protection methods in databases used in web applications to ensure reliable protection against unauthorized access and other types of cyber threats.

Objectives:

1. Study and analyze existing encryption and data protection methods.
2. Develop an efficient protection system based on modern technologies.
3. Select and adapt optimal tools and solutions for data protection.
4. Develop management and control strategies for the security system.
5. Conduct an analysis and evaluation of the effectiveness of the developed system.

Methods Used: Research on cryptographic protection methods, analysis of data security systems, development, and testing of the protection system.

Results Obtained:

During the work, a comprehensive data protection system for web applications was developed, including modern encryption and protection methods. Tools and solutions that allow efficient data security control and prevention of unauthorized access were successfully selected and integrated. The analysis results showed an increase in the level of system security and reliability, confirming the effectiveness of the chosen methods and approaches.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В эпоху цифровизации бизнеса, использование интернет-технологий стало краеугольным камнем для компаний различных масштабов. Интернет-сети применяются для обмена файлами, настройки частных виртуальных сетей и создания общедоступных ресурсов. Важнейшим направлением в этой области является разработка веб-приложений.

Веб-приложения - это системы, где взаимодействие между клиентом и сервером происходит через веб-браузер. Они имеют множество преимуществ, включая универсальность, совместимость с разными устройствами, а также простоту обновления для пользователей. Однако эти преимущества сопровождаются повышенными требованиями к качеству интернет-соединения и строгими мерами информационной безопасности.

Актуальность темы

Тема "Анализ методов шифрования и защиты баз данных в веб-приложениях" является крайне актуальной в свете увеличивающейся потребности защиты данных и операций пользователей в интернет-сервисах. В современном мире, где веб-приложения ежедневно обрабатывают огромные объемы заказов и финансовой информации, существует насущная необходимость в эффективных мерах безопасности. Важность этого обусловлена не только стремлением укрепить доверие клиентов, но и необходимостью соответствия законодательным стандартам по защите персональных данных.

Исследование сосредоточено на изучении различных подходов к обеспечению безопасности веб-приложений, что является ключевым аспектом в сохранении конфиденциальности и целостности пользовательских данных в сети.

Цель и задачи дипломной работы

Основная цель моей дипломной работы - глубокое исследование и анализ различных методик шифрования и защиты информации в базах данных, используемых в веб-приложениях. Я стремлюсь разработать действенные способы защиты данных клиентов и усовершенствовать безопасность операций в этих системах. Для достижения поставленной цели мной запланированы следующие конкретные задачи:

1. Сбор и детальный анализ требований к безопасности данных: Изучить существующие требования и стандарты, касающиеся безопасности информации в веб-приложениях.

2. Разработка модели безопасности: Создание комплексной модели безопасности, которая будет эффективно защищать данные в веб-приложениях.

3. Имплементация и проверка методов шифрования: Реализация и последующее тестирование выбранных техник шифрования и методов защиты данных.

4. Внедрение системы безопасности: Интеграция разработанной системы безопасности в уже существующую инфраструктуру веб-приложения.

5. Оценка результативности и надежности системы: Анализ эффективности и надежности внедренной системы безопасности в контексте реального использования веб-приложениями.

Целью этих действий является не только повышение уровня защищенности данных, но и укрепление доверия клиентов к веб-приложениям, а также соответствие современным требованиям в области информационной безопасности.

В качестве теоретико-методологических основ исследования в данной выпускной квалификационной работе рассматривается ряд литературных источников и научных работ – всего 10 источников. При решении поставленных задач в качестве основополагающих документов используются национальные и международные стандарты ISO.

Моя выпускная квалификационная работа структурирована на три основные части: теоретическую, аналитическую и проектную, каждая из которых играет ключевую роль в полном и всестороннем освещении темы "Анализ методов шифрования и защиты баз данных в веб-приложениях".

Обзор информационных систем и методов обеспечения безопасности WEB-приложений. Здесь я заложил основу для дальнейшего исследования, предоставив необходимые теоретические сведения. Она включает в себя определения и классификацию информационных систем, а также разбор различных уязвимостей и атак, специфичных для веб-приложений. Кроме того, в этом разделе я подробно рассмотрел и проанализировал существующие методы и инструменты, применяемые для обеспечения безопасности веб-приложений.

Разработка защищенного канала. Во втором разделе я провел глубокий анализ деятельности конкретной организации, что позволило мне выявить основные задачи и определить направления для разработки подсистемы защиты. Здесь были сформированы цели и назначение предстоящих разработок, а также обоснован выбор проектных решений,

наиболее подходящих для решения выявленных проблем безопасности в контексте деятельности организации.

Усовершенствование системы безопасности: анализ, разработка и оценка. В третьей части работы я сосредоточился на практической реализации теоретических и аналитических находок. Здесь описывается структура модернизированной базы данных, приводятся характеристики и функционал результирующей информационной системы. Также в этом разделе детально разбираются разработанные модули подсистемы безопасности после модернизации, их взаимосвязь и интерфейс, что дает полное представление о реализованных проектных решениях.

БИБЛИОГРАФИЯ

1. АРТЕМОВ А.В. *Информационная безопасность.* Орел: МАБИВ, 2014. 256 с. ISBN. 978-5-457-72324-5.
2. ВАСИЛЬКОВ, А. В. *Безопасность и управление доступом в информационных системах* / А.В. Васильков, И.А. Васильков. - М.:Форум, 2015. - 368 с. ISBN 978-5-91134-360-6.
3. ВОРА П. *Шаблоны проектирования веб-приложений* / П. Вора – М.: Эксмо,2011, – 870с. ISBN. 978-5-699-45019-0.
4. ГЕЙН А.А. *Web-программирование на PHP*. М.: ИНТУИТ.РУ «Интернет-университет информационных технологий». То же [Электронный ресурс]. - Disponibil: http://www.intuit.ru/department/internet/phpwebprog, 2016.
5. ДАРИ К. AJAX и PHP: *разработка динамических веб-приложений* / К. Дари, Б. Бринзаре, Ф. Черчез-Тоза, М. Бусика; пер. с англ. Киселева А. – Спб.:Символ-плюс, 2009, – 336с. ISBN 978-5-93286-077-4.
6. ДИГО С. М. *Проектирование и использование баз данных*: Учебник. - М.: Финансы и статистика, 2016. ISBN 978-5-374-00055-9.
7. ДЖОНС М. Т. *Программирование искусственного интеллекта в приложениях* /М. Тим Джонс; пер. с англ. Осипов А.И. – М.:ДМК Пресс,2015. – 312с. [63-68,82-83] ISBN 978-5-94074-746-8.
8. PECA L., ȚURCANU D. *Computer networks: Practical examples solved to be introduced in computer networks.* ISBN 978-9975-45-812-2. Chișinău, Publisher „Tehnica-UTM”, 2022. Dispomibil: http://repository.utm.md/bitstream/handle/5014/20549/Computer-networks-Practical-examples-DS.pdf?sequence=3&isAllowed=y
9. ȚURCANU D., SPINU N., POPOVICI S., ȚURCANU T. *Cybersecurity of the Republic of Moldova: a retrospective for the period 2015-2020.* Journal of Social Sciences, Vol. IV, no. 1 (2021), pp. 74 – 83. Disponibil: https://ibn.idsi.md/sites/default/files/imag_file/JSS-1-2021_74-83_0.pdf
10. PECA L., ȚURCANU D. *Network security: Practical examples solved to be introduced in network security.* Chișinău, Publisher „Tehnica-UTM”, 2023, pp. 7-232. Disponibil: http://repository.utm.md/bitstream/handle/5014/22819/Network-security-Practical-examples-Guide.pdf?sequence=1&isAllowed=y
11. ГОСТ 34.602-89. *Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.* Disponibil: https://b.eruditor.link/file/378618/

12. *Пиццерия Pizza9.md - в Кишиневе и пригородах.* https://pizza9.md/
13. ГОСТ 51583-2000. *Защита информации. Порядок создания автоматизированных систем в защищенном исполнении.* Disponibil: https://ridero.ru/books/zashishennye_avtomatizirovannye_sistemy/