НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Марценюк Б.В. (підпис)

УДК 004.891.3+681.5

ДОСЛІДЖЕННЯ ТА СТВОРЕННЯ МЕТОДІВ ШИФРУВАННЯ ПОВІДОМЛЕНЬ КОРИСТУВАЧА ВЕБ-СЕРВІСУ ДЛЯ ІНТЕРНЕТ ЛИСТУВАННЯ

Спеціальність 123.02М – Системне програмування

Науково-дослідна робота магістра

Харків – 2020

Дипломною роботою є рукопис.

Робота виконана на кафедрі «Обчислювальна техніка та програмування» Національного технічного університету «Харківський політехнічний інститут» Міністерства освіти і науки України.

Науковий керівник кандидат технічних наук, професор

(підпис) **Філоненко Алевтина Михайлівна**,
Національний технічний університет «Харківський політехнічний інститут», професор кафедри «Обчислювальна техніка та програмування»

Захист відбудеться «16» грудня 2020 р. о 9 годині на засіданні Державної екзаменаційної комісії у Національному технічному університеті «Харківський політехнічний інститут» за адресою: вул. Кирпичева, 2, м. Харків, 61000, вечірній корпус, ауд. 302.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Років десять тому листування через інтернет в основному використовувалось в розважальних цілях: чати, соціальні мережі та подібне. Але сьогодні інтернет листування ще й повноцінний інструмент роботи: вебінари і консультації по скайпу, рішення групових завдань у спільній розмові, обговорення батьками шкільних проблем, уточнення інформації при віддаленій роботі і навіть курси навчання в режимі онлайн.

Ринок запропонованих суспільству додатків, месенджерів, поштових клієнтів все більше і більше розвивається. Кожен користувач може обрати для себе найбільш зручний спосіб інтернет листування, або інтернет спілкування у цілому. Інтернет листування не закінчується на звичайних повідомленнях у вигляді тексту. Різноманітні голосові повідомлення, короткі відеозаписи вже стали для людства звичайною справою.

У сучасному інформаційному суспільстві велику загрозу конфіденційності та цілісності інформації представляє кіберзлочинність. Зростання кількості кібератак та доступність програмно-технічних засобів для їх реалізації зумовлює необхідність розробки сучасних засобів інформаційної безпеки громадян та держави в цілому.

Основною метою дипломного проекту є дослідження методів шифрування повідомлень користувача та розробка веб-сервісу для інтернет листування. Виходячи з поставленої цілі, були визначені задачі:

- дослідження існуючих методів шифрування повідомлень;
- проведення порівняння існуючих методів з метою виявлення недоліків та переваг кожного з них;
- дослідження існуючих методів хешування паролів;
- на основі проведених досліджень розробити веб-сервіс;
- досягти безпечного зберігання повідомлень на основі шифрування;
- розробити зручний інтерфейс для користувача;

Зв'язок роботи з науковими програмами, планами, темами. Робота виконана відповідно до плану науково-дослідних робіт кафедри обчислювальної техніка та програмування НТУ "ХПІ".

Мета і завдання дослідження. Метою дослідження є аналіз існуючих методів шифрування повідомлень користувача веб-сервісу інтернет листування. Виходячи з поставленої цілі, були визначені задачі:

- дослідження існуючих методів шифрування повідомлень;
- проведення порівняння існуючих методів з метою виявлення недоліків та переваг кожного з них;
- дослідження існуючих методів хешування паролів;
- на основі проведених досліджень розробити веб-сервіс;
- досягти безпечного зберігання паролів на основі шифрування;
- розробити зручний інтерфейс для користувача;
- проведення аналізу питань з охорони праці та навколишнього середовища;
- проведення оцінки конкурентоздатності.

Об'єктом дослідження є процес дослідження та створення методів шифрування повідомлень користувача веб-сервісу для інтернет листування

Предметом дослідження виступають методи шифрування повідомлень веб-сервісу, та їх переваги та недоліки.

Методи дослідження. Методика дослідження базується на аналізі відомих методів шифрування для виявлення основних недоліків та переваг, знаходження слабких сторін, дір у шифруванні приватних переписок серед схожих веб-сервісів.

Наукова новизна одержаних результатів полягає в наступному:

1. Було удосконалено метод наскрізного шифрування. На відміну від існуючого методу, у якому відбувається шифрування переписки за допомогою загального ключа для всіх учасників переписки, було запропоновано використовувати ключ унікальний для кожного учасника. За допомогою свого ключа повідомлення шифрується методом повторного хешування з доданням інших ключів

Практичне значення одержаних результатів дипломної роботи полягає у створенні, на основі поставлених в роботі вимог, працездатного веб-сервісу для інтернет листування.

Особистий внесок здобувача. Всі результати дипломного проектування, що виносяться на захист, отримані здобувачем особисто. Була розроблена власна модель веб-сервісу інтернет листування, запропоновано унікальний метод шифрування даних. Також було розроблено гнучкий веб-інтерфейс. Проведена аналітика та порівняння існуючих методів шифрування даних. В [1] здобувач провів аналіз безпеки бази даних та методів шифрування даних у хмарному сховищі.

Апробація результатів дипломної роботи. Основні положення дипломної роботи було викладено у вигляді статті у збірнику наукових праць “Системи управління, навігації та зв'язку, 2020, випуск 3(61)”.

Структура й обсяг роботи. Дипломна робота складається із вступу, шести розділів, висновків, списку використаних джерел інформації.

Основний зміст викладено на 81 сторінках тексту, містить 14 рисунків, 23 таблиці. Список використаних джерел налічує 34 найменування. Загальний обсяг 106 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовується актуальність теми дипломного проекту, його наукова і практична цінність, сформульовані мета і завдання роботи, наведена його загальна характеристика.

У першому розділі проведено аналіз існуючих методів шифрування повідомлень:

- симетричного шифрування;
- наскрізного шифрування;
- Діффі-Хелмана.

Наведено порівняння основних методів хешування паролів:

- методи категорії MD;
- методи категорії SHA.

У другому розділі було описано мору програмування Java, шаблон проектування MVC, описані технології проектування бази даних.

У третьому розділі описано процес розробки, а саме:

- розробка структури та проектування бази даних;
- розробка інтерфейсу користувача;
- розробка алгоритму шифрування переписки користувача;
- проектування серверної частини.

У четвертому розділі розглянуті питанні цивільного захисту населення. Описано сутність рятувальних та інших невідкладних робіт, рятування людей при надзвичайних ситуаціях, аварійно-рятувальних робіт внаслідок вибухів.

У п'ятому розділі розглянуті питання охорони праці та навколишнього середовища. Наведено перелік небезпечних та шкідливих виробничих факторів, які впливають на роботу інженерів-програмістів. Також було визначено оптимальні параметри мікро клімату і характеристику виробничого освітлення в приміщенні, дозволені рівні шуму та вібрації, статичної електрики та електромагнітних випромінювань. Розглянуто питання електробезпеки та пожежної безпеки.

У шостому розділі виконано техніко-економічне обґрунтування розробки (бізнес-план). Наведені економічні розрахунки собівартості розробки і тиражування програмного продукту. Також наведені результати маркетингових досліджень щодо вигідності розробки та продажу цього продукту. Розроблена стратегія просування продукту на ринку. Приведено фінансовий план та розрахунки точки беззбитковості проекту.

ВИСНОВКИ

У роботі вирішена науково-технічна задача створення веб-сервісу інтернет листування.

За результатами виконання поставлених задач та проведеної науково-дослідної роботи сформульовано такі висновки:

1. Проведено дослідження існуючих методів шифрування повідомлень, порівняння існуючих методів з метою виявлення недоліків та переваг кожного з них; проведено аналіз існуючих методів хешування паролів;

2. Проведено аналіз мов програмування. На основі аналізу було зроблено вибір на користь мови програмування Java як основної мови розробки, технології Swing як засіб створення графічного інтерфейсу та СУБД MySQL як засобу зберігання інформації.

3. У проектному розділі було виконано розробку бази даних, з описом усіх таблиць та їх призначення, розроблено інтерфейс користувача, створено власний алгоритм шифрування паролів для безпечного зберігання у базі даних, спроектовано серверну та клієнтську частину веб-сервісу.

4. Створений сервіс та компоненти системи відповідають заявленим функціональним і сучасним технічним вимогам і готові до широкого використання.

5. Розроблений програмний продукт розроблявся згідно з ДСТУ та відповідає вимогам технічного завдання.

6. Розглянуті питання охорони праці, а саме загальні питання з охорони праці, гігієна праці та виробнича санітарія, організація робочого простору, електробезпека в приміщеннях з ЕОМ, пожежна безпека.

СПИСОК ОСНОВНИХ ПУБЛІКАЦІЙ ЗА ТЕМОЮ ДИПЛОМОГО ПРОЕКТУ

1. Щербініна Є.М., Марценюк Б.В., к.т.н. проф. Філоненко А.М. // Database security and study of data encryption methods in Cloud Storage // Системи управління, навігації та зв'язку. Вип уск 3(61)// Полтава, 2020.

АНОТАЦІЯ

Марценюк Б.В. Дослідження та створення методів шифрування повідомлень користувача веб-сервісу для інтернет листування. – Рукопис.

Дипломна робота магістра за спеціальністю 123.02М – Системне програмування. – Національний технічний університет «Харківський політехнічний інститут», Харків, 2020.

Метою дослідження є дослідження методів шифрування повідомлень користувача та розробка веб-сервісу для інтернет листування.

У роботі проведено аналіз методів шифрування повідомлень користувача веб-сервісу інтернет листування, методів хешування паролів. Були проаналізовані недоліки та переваги кожного методу. Створена власна модель веб-сервісу інтернет листування з запропонованим методом шифрування повідомлень користувача.

Ключові слова: веб-сервіс для інтернет листування, шифрування, хешування.

АННОТАЦИЯ

Марценюк Б.В. Исследование и создание методов шифрования сообщений пользователя веб-сервиса для интернет переписки. – Рукопись.

Дипломная работа магистра по специальности 123.02М – Системное програмирование. – Национальный технический университет «Харьковский политехнический институт», Харьков, 2020.

Целью исследования является исследование методов шифрования сообщений пользователя и разработка веб-сервиса для интернет переписки.

Проведено исследование существующих методов шифрования сообщений, сравнение существующих методов с целью выявления недостатков и преимуществ каждого из них; проведен анализ существующих методов хеширования паролей. Проведен анализ языков программирования. На основе анализа был сделан выбор в пользу языка программирования Java как основного языка разработки, технологии Swing как средство создания графического интерфейса и СУБД MySQL как средства хранения информации. В проектном разделе были выполнены разработку базы данных, с описанием

всех таблиц и их назначения, разработаны интерфейс, создан собственный алгоритм шифрования паролей для безопасного хранения в базе данных, спроектировано серверную и клиентскую часть веб-сервиса.

Созданный сервис и компоненты системы соответствуют заявленным функциональным и современным техническим требованиям и готовы к широкому использованию. Разработанный программный продукт разрабатывался по ГОСТ и соответствует требованиям технического задания. Рассмотрены вопросы охраны труда, а именно общие вопросы по охране труда, гигиена труда и производственная санитария, организация рабочего пространства, электробезопасность в помещениях с ЭВМ, пожарная безопасность.

Ключевые слова: веб-сервис для интернет-переписки, мессенджеры, клиент-сервер.

ABSTRACT

Martseniuk B.V. Research and creation of methods for encrypting messages of a web service user for Internet correspondence. – Manuscript.

Master's Thesis in the specialty 123.02M – System programing. – National Technical University " Kharkiv Polytechnic Institute", Kharkov, 2020.

The aim of the research is to study methods of encrypting user messages and develop a web service for Internet correspondence.

The paper analyzes methods of encrypting messages of a user of a web service of Internet correspondence, methods of hashing passwords. The advantages of each method were also analyzed. Created its own model of the Internet correspondence web service with the proposed method of encrypting user messages.

Key words: web service for Internet correspondence, encryption, hashing.