

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧОРНОМОРСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ПЕТРА МОГИЛИ

Нікітін Сергій Олександрович

УДК 004.925.5

**ПРОГРАМНА СИСТЕМА РОЗПІЗНАВАННЯ
ЦИФРОВОГО ПІДПISУ**

Напря́м підготовки 6.050102 – Комп'ютерна інженерія

Автореферат
бакалаврської роботи
на здобуття кваліфікації бакалавра з комп'ютерної інженерії

Миколаїв – 2019

Робота виконана у Чорноморському національному університеті ім. Петра Могили.

Керівник: доктор технічних наук, професор
Гожий Олександр Петрович,
ЧНУ ім. Петра Могили,
професор кафедри комп'ютерної інженерії

Рецензент: канд. фіз.-мат. наук
Кулаковська Інеса Василівна,
ЧНУ ім. Петра Могили,
доцент кафедри інтелектуальних
інформаційних систем

Консультант: д-р біол. наук, професор
Григор'єва Людмила Іванівна,
ЧНУ ім. Петра Могили,
Зав. кафедри екології Медичного інституту, професор

Захист відбудеться « 26 » червня 2019 р. о 10-00 на засіданні
Державної екзаменаційної комісії в ЧНУ ім. Петра Могили, ауд. 2-406

З бакалаврською роботою можна ознайомитись на сайті ЧНУ ім. Петра Могили
за посиланням <http://chmnu.edu.ua>

Автореферат оприлюднений « 18 » червня 2019 р.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Проблема збереження та використання електронних документів від копіювання, модифікації і підробки вимагає для свого вирішення специфічних засобів і методів захисту. Одним з поширених в світі засобів такого захисту є *Електронний цифровий підпис* (ЕЦП), який за допомогою спеціального програмного забезпечення підтверджує достовірність інформації документу, його реквізитів і факту підписання конкретною особою.

Програми електронного документообігу з використанням ЕЦП на сьогодні активно впроваджується в державних установах і органах державної влади, що істотно розширює можливості застосування ЕЦП і розвиток електронного документообігу в Україні. Тому тема дипломної роботи є *актуальною* у сучасних умовах.

Електронний цифровий підпис спрямований на спрощення та прискорення документообігу між суб'єктами господарювання, що, в свою чергу, має зміцнити конкурентоспроможність вітчизняних підприємств, адже пришвидшиться процедура укладення цивільно-правових та господарських договорів, оформлення експортно-імпортних операцій, надання електронних банківських послуг. Електронний цифровий підпис призначено для: ідентифікації особистості, дистанційної ідентифікації, забезпечення безпечності ідентифікації, юридичного підтвердження особистості. Отже, ЕЦП - це сучасний спосіб підпису документів.

Розвитком теорії та практики впровадження систем шифрування та розпізнавання цифрового підпису займалися такі провідні вчені, як: Горбенко І.Д., Домарєв В.В., а також Брюс Шнайер, Філіп Циммерманн та інші.

Метою дипломної роботи є вдосконалення процесу розпізнавання, завдяки модифікації алгоритму розпізнавання цифрового підпису.

Для досягнення мети в бакалаврській роботі поставлені та вирішені наступні **задачі**:

- Дослідити сучасні схеми створення електронного цифрового підпису та провести порівняльний аналіз найбільш поширених схем;
- За результатами аналізу виявити фактори, що впливають на швидкодію, та запропоновано оптимізований алгоритм;
- Підібрати апаратні компоненти для ефективної роботи програмної системи розпізнавання цифрового підпису;
- Розробити програмну систему розпізнавання цифрового підпису;
- Проаналізувати засоби для забезпечення вимог охорони праці при роботі в приміщенні інформаційно-обчислювального відділу МФ ТОВ «Преса».

Об'єкт: процес модифікації та вдосконалення алгоритму розпізнавання цифрового підпису на основі алгоритму DSA.

Предмет: алгоритми в системах ідентифікації цифрового підпису.

Використані методи: криптографії, методи та алгоритми асиметричного шифрування, методи об'єктно-орієнтованого підходу в процесі розроблення програмних засобів.

Результатом даної **роботи** є розробка програмної системи цифрового підпису, яка дозволяє створювати цифровий підпис та ідентифікувати його, за допомогою актуальних алгоритмів.

Структура та обсяг роботи. Бакалаврська робота складається з анотації на 2 сторінках, вступу, чотирьох розділів, висновків, переліку джерел посилання з 33 найменувань, 1 додатку на 7 сторінках. Основна частина роботи становить 66 сторінок, серед яких 12 рисунків та 3 таблиці

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** подано обґрунтування актуальності теми бакалаврської роботи, сформульовано мету та основні завдання, визначено практичне значення отриманих результатів. Задача побудови програмного забезпечення для розпізнавання цифрового підпису набуває своєї актуальності разом з розвитком

програмних та апаратних засобів ідентифікації особистості та електронного документообігу.

У першому розділі бакалаврської роботи «Аналітичний огляд розробок у сфері проектування систем розпізнавання цифрового підпису» проведено огляд існуючих розробок у сфері проектування та використання систем розпізнавання цифрового підпису, що дало змогу визначити основні вимоги до системи, що розробляється.

В результаті аналізу було виявлено, що ЕЦП набуває все більшого поширення в організаціях. Тим не менше в процесі застосування ЕЦП в діяльності організацій виникає ряд проблем: необхідність постійного вдосконалення алгоритмів; невирішеність проблеми довготривалого зберігання; обмеження сфери використання; відсутність необхідності застосування ЕЦП в закритих інформаційних системах.

В розділі акцентується увага на різницях понять звичайного та електронного підпису, перелічуються переваги електронного цифрового підпису перед звичайним. А також дається огляд галузей призначення ЕЦП. Все це дало можливість сформулювати основні вимоги до цифрового підпису.

Розглянуто сукупність схем побудови цифрового підпису, які поділяються на дві основні групи: на основі алгоритмів симетричного шифрування та на основі алгоритмів асиметричного шифрування. Крім цього, існують інші різновиди цифрових підписів (груповий підпис, незаперечний підпис, довірений підпис), які є модифікаціями описаних вище схем. Їх поява обумовлена різноманітністю завдань, що вирішуються за допомогою ЕЦП. Детальний аналіз переваг та недоліків кожної схеми побудови цифрового підпису дало можливість зупинитись в процесі розробки програмної системи на схемі використання алгоритмів асиметричного шифрування.

Асиметричні схеми ЕЦП відносяться до криптосистем з відкритим ключем. На відміну від симетричних алгоритмів шифрування, в яких шифрування та дешифрування проводиться за допомогою єдиного ключа, у схемах цифрового

підпису підписування проводиться із застосуванням закритого ключа, а перевірка - із застосуванням відкритого. Схема формування асиметричного цифрового підпису представлена на рис.1.

Важливою проблемою всієї криптографії є управління ключами. Ключі поділяються на відкриті та закриті. Розглядається особливість керування кожного виду ключів.

В розділі також представлені порівняльний аналіз захищених ключових носіїв різних виробників, огляд протоколів та стандартів цифрового підпису.

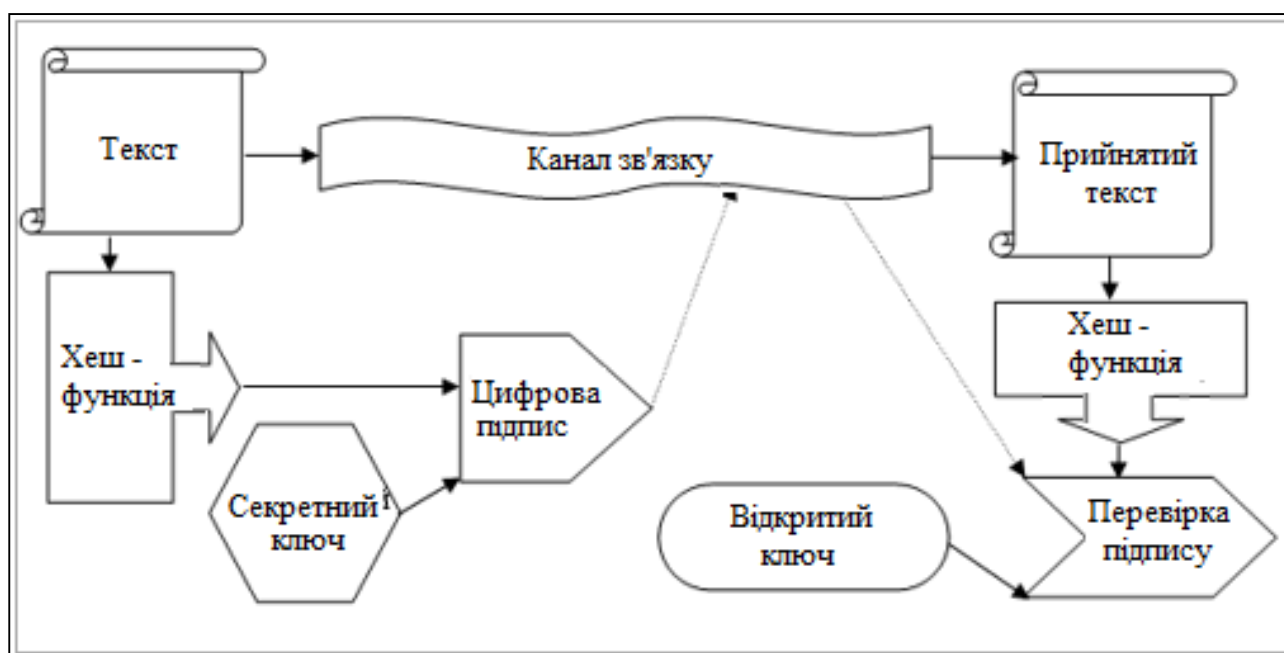


Рисунок 1 - Схема формування асиметричного ЕЦП

У другому розділі бакалаврської роботи «Розробка апаратної частини для системи розпізнавання цифрового підпису» здійснюється вибір апаратної частини для коректної роботи програмної системи розпізнавання цифрового підпису.

Апаратна реалізація забезпечує захищеність процесу виконання криптографічних перетворень та унеможливорює доступ до особистих ключів з боку апаратного-програмного середовища.

Розглянуто крипто модулі типу «Грядя-61» та «Грядя-301». Наведено основні характеристики та особливості використання.

Апаратна реалізація мережного криптомодуля забезпечує захищеність виконання усіх криптографічних перетворень усередині модуля та унеможливорює доступ до особистих ключів з боку апаратного-програмно середовища.

Особисті ключі генеруються, зберігаються та використовуються тільки у середині мережного криптомодуля, та жодним способом не потрапляють за його межі. Зберігання особистих ключів та інших ключових даних здійснюється у постійному запам'ятовуючому пристрої мережного криптомодуля (його внутрішнього криптомодуля).

У третьому розділі бакалаврської роботи «Розробка програмної частини для системи розпізнавання цифрового підпису» описано процес проведення розробки програмного забезпечення (ПЗ) для вирішення задачі розпізнавання цифрового підпису. Обґрунтовано вибір середовища та мови програмування для розробки програмного забезпечення. ПЗ розроблено мовою *Java* в середовищі *IDE NetBeans*.

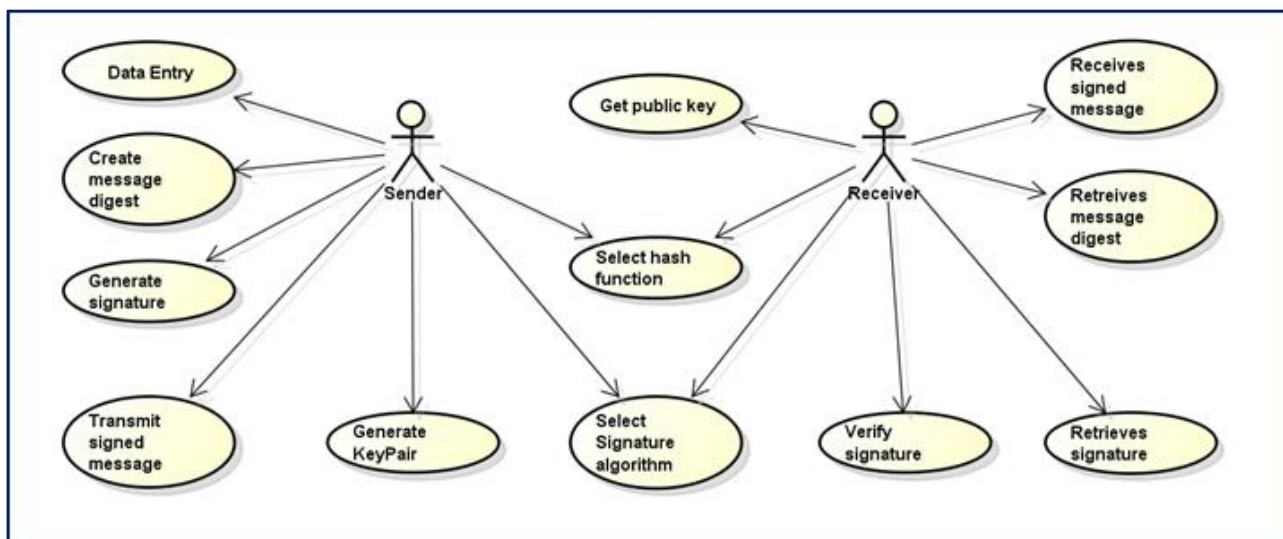


Рисунок 2 - Діаграма варіантів використання

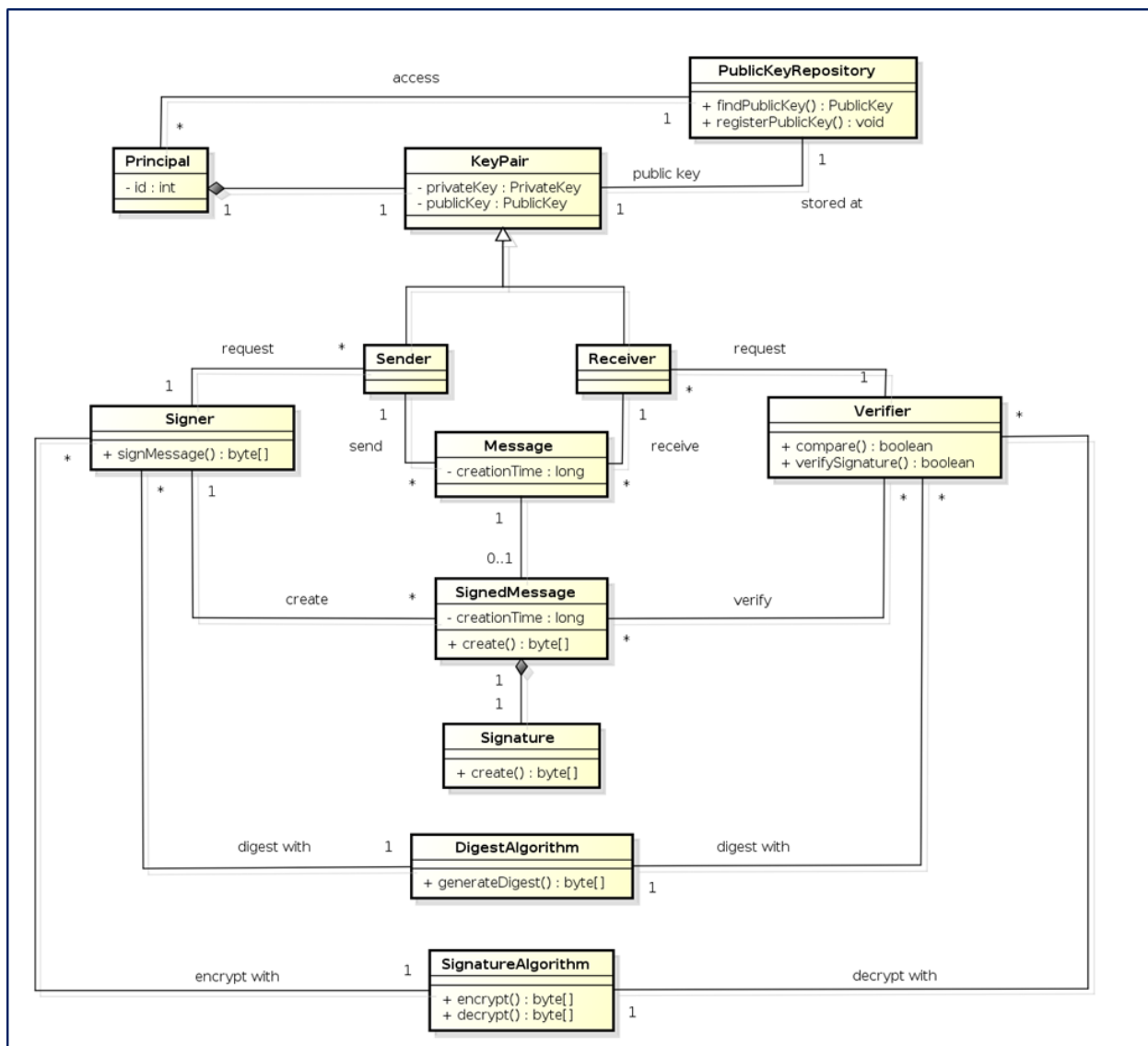


Рисунок 3 - Діаграма класів

Для проектування програмного забезпечення було розроблено UML діаграми. На рис. 2 наведено діаграма варіантів використання, а на рис. 3 – діаграма класів. Усі діаграми в роботі були побудовані за допомогою спеціалізованого середовища UML-проектування *Astah Professional*. За допомогою UML діаграм встановлено, які функції реалізовано у програмному забезпеченні, та яким чином елементи системи взаємодіють між собою.

На рис. 4-7 наведені основні екранні форми, розробленого програмного забезпечення, які демонструють основні функції ПЗ.

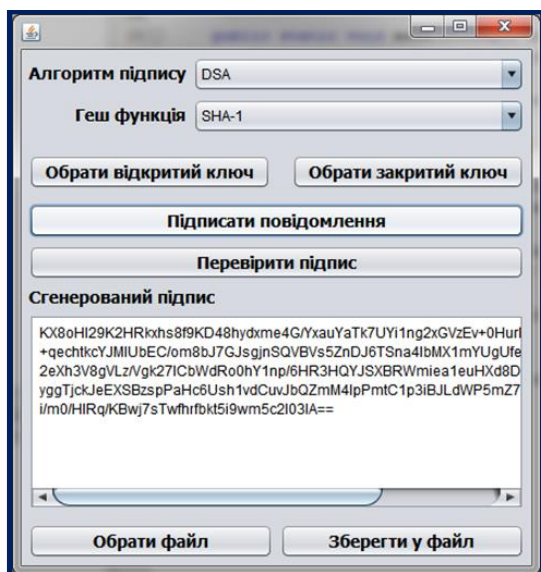


Рисунок 4 - Створення цифрового підпису повідомлення

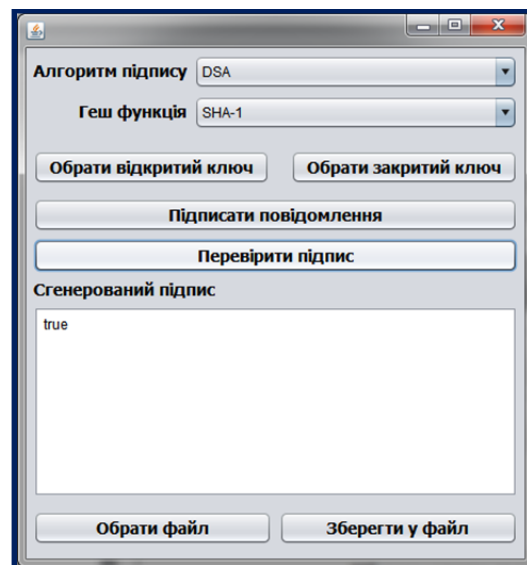


Рисунок 5 - Перевірка підпису

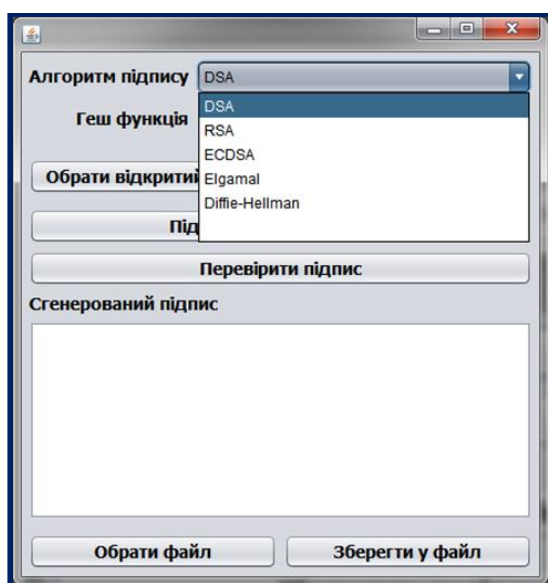


Рисунок 6 - Обрання алгоритму підпису

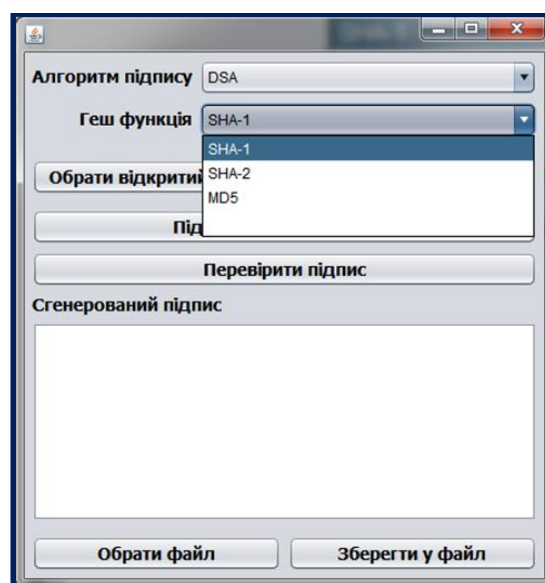


Рисунок 7 - Обрання алгоритму хеш-функції

Додаток містить лістинг коду ПЗ для розпізнавання цифрового підпису.

У спеціальній частині «Охорона праці» наведено аналіз засобів для забезпечення вимог охорони праці при роботі в приміщенні інформаційно-обчислювального відділу МФ ТОВ «Преса». Встановлено відповідність всіх розглянутих показників чинним санітарним нормам та виявлено, що умови праці в МФ ТОВ «Преса» є оптимальними.

ВИСНОВКИ

В результаті виконання дипломної роботи:

1. На основі проведеного аналітичного огляду сучасних схеми створення електронного цифрового підпису, виявлене основні вимоги до програмної системи розпізнавання цифрового підпису.
2. За результатами аналізу виявлене фактори, що впливають на швидкодію алгоритму, що є основою програмної системи. Запропоновано та реалізовано оптимізований алгоритм розпізнавання цифрового підпису.
3. Здійснено підбір компонентів апаратної частини для ефективної роботи програмної системи розпізнавання цифрового підпису.
4. Розроблено програмна система розпізнавання цифрового підпису, що виконує такі функції: створення цифрового підпису повідомлення, перевірка підпису, обрання алгоритму підпису, обрання алгоритму хеш-функції, обрання відкритого/закритого ключа.
5. У спеціальному розділі з охорони праці наведено аналіз засобів для забезпечення вимог охорони праці при роботі в приміщенні інформаційно-обчислювального відділу МФ ТОВ «Преса».

Отже, електронний цифровий підпис спрямований на спрощення та прискорення документообігу між суб'єктами господарювання, що, в свою чергу, має зміцнити конкурентоспроможність вітчизняних підприємств, адже пришвидшиться процедура укладення цивільно-правових та господарських договорів, оформлення експортно-імпортних операцій, надання електронних банківських послуг.

АНОТАЦІЯ

Нікітін С.О. Програмна система розпізнавання цифрового підпису. - Кваліфікаційна робота бакалавра з напрямку підготовки 123 - Комп'ютерна інженерія на здобуття кваліфікації «фахівець з інформаційних технологій». – Чорноморський національний університет імені Петра Могили, 2019.

Бакалаврська робота спрямована на дослідження та розробку програмної системи розпізнавання цифрового підпису. Результатом роботи є розробка програмної системи цифрового підпису, яка дозволяє створювати цифровий підпис та ідентифікувати його, за допомогою актуальних алгоритмів.

Пояснювальна записка бакалаврської роботи складається зі вступу, трьох розділів, висновків, переліку джерел посилання, 1 додатку та спеціальної частини з охорони праці.

У вступі визначається актуальність теми, наведені задачі, які заплановано вирішити для досягнення поставленої мети. У першому розділі проводиться аналіз існуючих розробок у сфері проектування та використання систем розпізнавання цифрового підпису, визначаються основні вимоги до системи, що розробляється. У другому розділі здійснюється вибір апаратної частини для коректної роботи програмної системи розпізнавання цифрового підпису. У третьому розділі надається опис розробки програмного забезпечення (ПЗ) для вирішення задачі розпізнавання цифрового підпису. ПЗ розроблено мовою Java в середовищі IDE NetBeans. У висновках наводяться підсумки проведеної роботи та основні переваги розробленої системи перед аналогами.

У спеціальній частині з охорони праці наведено аналіз засобів для забезпечення вимог охорони праці при роботі в приміщенні інформаційно-обчислювального відділу МФ ТОВ «Преса».

Бакалаврська робота містить 66 с. (без додатків), 12 рисунків, 3 таблиці, 33 джерел посилання та 1 додатку.

Ключові слова: цифровий підпис, електронний цифровий підпис, відкритий ключ, закритий ключ, хеш функція, алгоритм підпису.

ABSTRACT

Nikitin S.O. Software system for digital signature recognition. - Bachelor's thesis in the field of study 123 - Computer engineering. – Petro Mohyla Black Sea National University, 2019.

Bachelor's work is aimed at researching and developing a software system for digital signature recognition. The result of the work is the development of a software digital signature system, which allows you to create a digital signature and identify it, using current algorithms.

The thesis consists of an introduction, three chapters, conclusions, references, two appendices and a special chapter which covers problems of health and safety in emergency.

The introduction determines the relevance of the topic, sets out the tasks that are scheduled to be solved to achieve the goal. The first section analyzes the existing developments in the design and use of digital signature recognition systems, and defines the basic requirements for the system being developed. The second section chooses the hardware part for the correct operation of the digital signature recognition software system. The third section provides a description of the software development (software) for solving the problem of digital signature recognition. The software is developed in Java language in the NetBeans IDE environment. The conclusions give the results of the work performed and the main advantages of the developed system before the analogues.

In the special section on labor protection, the analysis of means for ensuring the requirements of labor protection at work in the premises of the Information and Computing Department of MF LLC «Press» is provided.

Thesis contains 66 p. (without appendices), 12 figures, 3 tables, 33 sources of reference and 1 application.

Keywords: digital signature, electronic digital signature, public key, private key, hash function, signature algorithm.