ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
(повне найменування вищого навчального закладу)
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ
(повне найменування інституту, назва факультету (відділення))
КАФЕДРА ПРОГРАМНИХ ЗАСОБІВ І ТЕХНОЛОГІЙ
(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи
магістра
(рівень вищої освіти)

на тему: «Дослідження методів шифрування та розробки електронного підпису»

Виконав: студент 6 курсу, групи 6ПР
спеціальності
121 «Інженерія програмного забезпечення»
(шифр і назва напряму підготовки, спеціальності)

Каспер Антон Володимирович_____.
(прізвище та ініціали)

Керівник к.т.н., доцент Огнєва О.Є.____
(прізвище та ініціали)

Рецензент к.т.н., доц.Вишемирська С.В.
(прізвище та ініціали)

Херсон – 2021р.

АНОТАЦІЯ

Кваліфікаційна робота магістра містить такі структурні частини: вступ, три розділи, висновок та список посилань.

Перший розділ «Дослідження методів, моделей, алгоритмів та методик шифрування електронного підпису та роботи із ним» складається з чотирьох частин: «Електронний підпис як елемент інформаційної безпеки», «Особливості електронного підпису та переваги його застосування», «Існуючі методи, моделі, алгоритми та методики шифрування електронного підпису» та «Існуючі методи, моделі, алгоритми та методики роботи з електронним підписом». У цьому розділі аналізується предметна область дослідження. Приводяться приклади існуючих методів і інформаційних систем електронного підпису.

У другому розділі «Дослідження інформаційних технологій та програмних продуктів для шифрування електронного підпису та роботи із ним» розміщено наступні підрозділи: «Програмні комплекси. які використовуються в засвідчуваних центрах та центрах сертифікації ключів», «Підписування електронних документів різних форм» та «Існуючі програмні продукти для шифрування та роботи з електронним підписом». У цьому розділі розглянуто технології, методи, моделі, алгоритми та методики для роботи з електронним підписом, описано основні методи та технології шифрування електронного підпису.

У третьому розділі «Проектування додатку для генерування та роботи з електронним підписом» розміщено наступні підрозділи: «Використання існуючих засобів та моделей для роботи та генерації електронного підпису», «Опис та побудова схем та моделей шифрування електронного підпису та роботи із ним», «Аналіз алгоритму шифрування SHA256» та «Постановка та обґрунтування проблеми». У цьому розділі описано використаний алгоритм шифрування електронного підпису, наведено підстави на розробку додатку.

Четвертий розділ «Розробка додатку та опис його функціонування» складається з п’яти підрозділів: «Опис модулів розроблюваного додатку», «Опис алгоритму генерації сертифікату електронного підпису та роботи з ним», «Тестування додатку», «Аналіз отриманих результатів» та «Вдосконалення додатку для генерації та роботи з електронним підписом». У цьому розділі наведено реалізацію програмного продукту. Приведено роботу кожного модуля, проведено тестування продукту.

ANNOTATION

The master's thesis contains the following structural parts: introduction, three sections, conclusion and list of references.

The first section "Research of methods, models, algorithms and methods of electronic signature encryption and work with it" consists of four parts: "Electronic signature as an element of information security", "Features of electronic signature and benefits of its use", "Existing methods, models, algorithms and methods of electronic signature encryption "and" Existing methods, models, algorithms and methods of working with electronic signatures ". This section analyzes the subject area of research.

The second section "Research of information technology and software products for electronic signature encryption and work with it" contains the following sections: "Software packages for certification centers of keys ," Signing of electronic documents of various forms" and "Existing software products for encryption and work with electronic signatures". This section describes the basic methods and technologies of electronic signature encryption.

The third section "Designing an application for generating and working with electronic signatures" contains the following sections: "Using existing tools and models for working with electronic signatures", "Description and construction of schemes and models for encrypting electronic signatures and working with it", "Analysis encryption algorithm SHA256 ". This section describes the algorithm used to encrypt the electronic signature.

The fourth section "Development of the application and description of its operation" consists of five sections: "Description of modules of the developed application", "Description of the algorithm for generating and working with electronic signature certificate", "Testing the application", "Analysis of results" and "Improvement application for working with electronic signatures". This section describes the implementation of the software product. The work of each module is given, product testing is carried out.

РЕФЕРАТ

Кваліфікаційна робота магістра: 107 сторінок, 47 рисунків, 4 таблиці, 52 джерела.

Мета роботи – розроблення додатку для роботи із електронним підписом. Для реалізації поставленої задачі необхідно проаналізувати особливості шифрування ЕП та основи кібербезпеки.

Об'єкт дослідження – метод підтвердження документів електронним підписом. Також розглядається проблема шифрування ЕП.

Предмет дослідження – дослідження методів шифрування та розробки електронного підпису.

Результат роботи: Розроблений додаток дасть можливість працювати із електронними документами та підтверджувати особу за допомогою підпису. Це концепція, яка допоможе покращити безпеку при роботі з сертифікатами цифрового підпису і використовувати її основи для подальших реалізацій та застосування.

Новизна роботи: Вперше досліджено особливості публічного та приватного ключа у цифровому сертифікаті. Розглянуто алгоритми генерування та шифрування електронного підпису.

Адаптовано роботу продукту до інших програмних засобів.

Реалізовано алгоритм, що забезпечує реалізацію електронного підпису для роботи з електронними документами.

Ключові слова: Додаток, електронний підпис, кібербезпека, шифрування даних.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

Скорочення, термін, позначення	**Пояснення**
ЕП	Електронний підпис
ЦП	Центральний процесор
API	*application programming interface*
DOCX	Microsoft Word Open XML Document.
PDF	Portable document format
PEM	Privacy Enhanced Mail Certificate
QA	*Quality Assurance*
RSA	Rivest, Shamir and Adleman
WPF	Windows Presentation Foundation
XML	eXtensible Markup Language

ЗМІСТ

ВСТУП

На сьогоднішній день актуальність електронного підпису набирає великих обертів, тому що її використання має широкі перспективи впровадження у всіх сферах життя сучасного суспільства, пов'язаних із передачею та обробкою інформації. За допомогою електронного підпису можна скористатися державними послугами різних відомств, не виходячи з дому, а також підписати електронні документи будь-якої складності, використати можливість ідентифікувати будь-яку людину за її ЕЦП за необхідності [1].

Основними перевагами використання електронного підпису в сучасному світі є швидкість, надійність, уникнення традиційного паперового документообігу, незалежність від територіальної розподільності сторін угоди.

Актуальність теми. На даний момент використання електронного підпису є необхідністю для отримання певних послуг та можливостей. Розроблюваний додаток наддасть можливості створювати сертифікат цифрового підпису та підтверджувати особу за допомогою створеного електронного підпису та взаємодіяти з іншими продуктами для роботи з документами.

Актуальність теми дослідження обумовлена наступними чинниками:

– Можливість працювати із електронними документами дистанційно;

– Можливість отримувати державні та комерційні послуги дистанційно;

– Недостатній набір готових програмних продуктів для роботи та генерування електронного підпису;

– Узагальнення накопиченого досвіду роботи з сертифікатами підпису;

Мета і задачі дослідження. Метою дослідження є розробка додатку для роботи та генерування електронного підпису. Для адаптації додатку необхідно дослідити можливості взаємодії з іншими програмними продуктами. Для реалізації поставленої задачі необхідно проаналізувати особливості шифрування ЕП та основи кібербезпеки.

Для досягнення поставленої мети необхідно виконати ряд **задач**:

– Вивчення особливостей створення електронного підпису;

– Вивчення методів, методик та моделей шифрування та створення електронного підпису;

– Вивчення особливостей шифрування та створення криптографічного ключа;

– Дослідження існуючих програмних продуктів для роботи та генерування електронного підпису;

– Проектування задачі створення сертифікату та підтвердження документів електронним підписом;

– Реалізація взаємодії додатку з електронними документами;

– Написання та реалізація програмного забезпечення;

– Тестування отриманих результатів.

Завдання, які було виконано під час дослідження:

– Проаналізувати існуючі програмні продукти для роботи та генерування електронного підпису;

– Дослідити особливості шифрування та створення електронного підпису;

– Запроектувати та розробити задачі створення сертифікату та підтвердження документів електронним підписом;

– Визначити напрямок адаптації додатку для роботи з документами різного типу;

– Адаптувати додаток під поставлені задачі;

– Реалізувати тестування програмного забезпечення.

Об’єкт дослідження – метод підтвердження документів електронним підписом. Також розглядається проблема шифрування та створення криптографічного ключа для ЕП.

Предмет дослідження – дослідження методів шифрування та розробки електронного підпису.

Новизна роботи: В результаті проведеного дослідження одержані наступні наукові результати:

— Досліджено особливості публічного та приватного ключа у цифровому сертифікаті.

— Розглянуто алгоритми генерування та шифрування електронного підпису.

— Адаптовано роботу додатку до інших програмних засобів.

— Реалізовано алгоритм, що забезпечує реалізацію електронного підпису для роботи з електронними документами.

— Розроблено додаток для роботи з документами та підтвердження за допомогою електронного підпису.

Практичне значення одержаних результатів. Розроблений додаток дасть можливість працювати із електронними документами та підтверджувати особу за допомогою підпису. Це концепція, яка допоможе покращити безпеку при роботі з сертифікатами цифрового підпису і використовувати її основи для подальших реалізацій та застосування.

Теоретичне значення одержаних результатів. Дослідження особливостей роботи електронного підпису матиме вагому роль у розвитку теми кібербезпеки у майбутньому. Можливість розуміти ключові особливості цієї теми допоможе також у сфері надання електронних послуг.

Апробація результатів бакалаврської кваліфікаційної роботи. Представлений програмний додаток може використовуватися для подальшого забезпечення електронної ідентифікації за допомогою ЕП. Одержані результати можна використовувати для удосконалення методики та інструментарію для створення подібних продуктів, запропонований додаток використовувати для подальшого використання цієї методики.

Публікації:

1. Каспер А.В., Огнєва О.Є. «Дослідження методів шифрування для розробки електронного підпису»/ Матеріали III всеукраїнської науково-технічної конференції «Інформаційні технології та програмування», http://kntu.net.ua/ukr/content/view/full/51654

2. Каспер А.В., Огнєва О.Є. «Додаток для генерування електронного підпису на основі методу шифрування x509» / Матеріали III всеукраїнської науково-технічної конференції «Інформаційні технології та програмування», http://kntu.net.ua/ukr/content/view/full/51654

Структура: робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел, додатків. Загальний обсяг роботи – 107 сторінок.