

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Факультет систем управління літальних апаратів

Кафедра комп'ютерних наук та інформаційних технологій

Пояснювальна записка
до кваліфікаційної роботи
(тип кваліфікаційної роботи)

магістра
(освітній ступінь)

на тему «Розробка апаратного ключа для захисту інформації в медичній
інформаційній системі»

XAI.302.367.23O.122.10685131 ПЗ

Виконав: студент 6 курсу групи № 367
Спеціальність 122 «Комп'ютерні науки»

(код та найменування)

Освітня програма Комп'ютеризація
обробки інформації та управління

Соколов А. В.

(прізвище й ініціали студента)

Керівник: Малєєва Ю. А.

(прізвище й ініціали)

Рецензент: Чалий С. Ф.

(прізвище й ініціали)

Міністерство освіти і науки України
Національний аерокосмічний університет ім. М.Є. Жуковського
«Харківський авіаційний інститут»

Факультет систем управління літальних апаратів
 Кафедра комп'ютерних наук та інформаційних технологій
 Рівень вищої освіти другий (магістерський)
 Галузь знань 12 «Інформаційні технології»
 (код та найменування)
 Спеціальність 122 «Комп'ютерні науки»
 Освітня програма Комп'ютеризація обробки інформації та управління

ЗАТВЕРДЖУЮ

Завідувач кафедри

Олег ФЕДОРОВИЧ

(підпис)

(ім'я та прізвище)

« 07 » листопада 2023 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТА

Соколова Анатолія Вячеславовича

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи Розробка апаратного ключа для захисту інформації в медичній інформаційній системі

керівник кваліфікаційної роботи Малєєва Юлія Анатоліївна, к.т.н, доцент,
 (прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом Університету № 1968-уч. від « 06 » листопада 2023 року.

2. Термін подання студентом кваліфікаційної роботи 10.01.2024.

3. Вихідні дані до проекту (роботи) відомості про організацію доступу до існуючих МІС; відомості про існуючі апаратні та програмні засоби забезпечення захищеного з'єднання з віддаленим сервером

4. Зміст пояснювальної записки (перелік завдань, які потрібно розв'язати) аналіз особливостей забезпечення захисту інформації в медичних інформаційних системах; аналіз існуючих рішень для захищеного з'єднання між користувачем та віддаленим сервером; проектування сценаріїв взаємодії користувача та застосунку для захисту інформації; розробка бази даних застосунку; проектування архітектури застосунку; розробка апаратного ключа для захисту з'єднання з медичною інформаційною системою; опис основних режимів роботи застосунку.

5. Перелік графічного матеріалу Розробка апаратного ключа для захисту інформації в медичній інформаційній системі; Актуальність розробки додатка для захисту інформації в медичній інформаційній системі; МІС «Каштан»; МІС «HELSI»; МІС «Облік кадрів України та пацієнтів»; Порівняння існуючих МІС; Аналіз інструментальних рішень з захисту інформації; Сценарії взаємодії користувача та застосунка; Структура БД апаратного ключа для захисту інформації в МІС; Архітектура комплексу по встановленню захищеного з'єднання з МІС; Приклад роботи веб-додатку адміністратора серверу підключень; Приклад роботи застосунку користувача; Висновки.

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
з основної частини	Малєєва Ю.А., доц. каф. 302		
зі спеціального розділу	Малєєва Ю.А., доц. каф. 302		
з економіки та управління	Малєєва Ю.А., доц. каф. 302		

Нормоконтроль _____ Олександр ПРОХОРОВ «____» _____ 2024 р.
(підпис) (ім'я та прізвище)

7. Дата видачі завдання «_06_» _вересня_ 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз існуючих підходів і інструментальних рішень захисту інформації в медичних системах	06.09-20.09	
2	Аналіз інструментальних рішень з захисту інформації	21.09 – 28.09	
3	Проектування ключа для захисту інформації в медичній інформаційній системі	29.09 – 20.11	
4	Опис особливостей реалізації апаратного ключа для захисту інформації в медичній інформаційній системі	21.11 – 20.12	
5	Опис роботи застосунку для захисту інформації в медичній інформаційній системі	21.12-22.12	
6	Економічний розділ	20.12 – 24.12	
7	Висновки та оформлення пояснювальної записки	24.12-25.12	

Студент _____ Анатолій СОКОЛОВ
(підпис) (ім'я та прізвище)

Керівник кваліфікаційної роботи _____ Юлія МАЛЄЄВА
(підпис) (ім'я та прізвище)

УДК 004.9

РЕФЕРАТ

Розробка апаратного ключа для захисту інформації в медичній інформаційній системі – Соколов Анатолій, кваліфікаційна робота магістра, Харків, Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», кількість сторінок, включаючи додатки 104, кількість таблиць 25, кількість рисунків 37, кількість джерел літератури 27.

КЛЮЧОВІ СЛОВА: апаратний ключ, захист даних, встановлення захищеного з'єднання, медична інформаційна система.

МЕТА РОБОТИ: надання можливості встановлення захищеного з'єднання між користувачем та віддаленим сервером медичної інформаційної системи.

ОБ'ЄКТ ДОСЛІДЖЕННЯ: процес створення захищеного з'єднання між користувачем та віддаленим сервером медичної інформаційної системи.

ПРЕДМЕТ ДОСЛІДЖЕННЯ: методи і технології встановлення захищеного з'єднання з віддаленим сервером медичної інформаційної системи.

ЗАДАЧІ ДОСЛІДЖЕННЯ: проаналізувати особливості забезпечення захисту інформації в медичних інформаційних системах; проаналізувати існуючі рішення для захищеного з'єднання між користувачем та віддаленим сервером; спроектувати сценарії взаємодії користувача та застосунку для захисту інформації; розробити базу даних застосунку; спроектувати архітектуру застосунку; розробити апаратний ключ для захисту з'єднання з медичною інформаційною системою; описати основні режими роботи застосунку.

МЕТОДИ ДОСЛІДЖЕННЯ: інформаційні технології та методи розробки застосунків та захисту з'єднань для ОС Windows, методи розробки веб-додатків.

ОТРИМАНІ РЕЗУЛЬТАТИ: створено апаратний ключ, який підвищує надійність захищеного з'єднання між користувачем та віддаленим сервером медичної інформаційної системи.

UDC 004.9

ABSTRACT

Development of a hardware key to protect information in the medical information system – Sokolov Anatoly, Master's Thesis, Kharkiv, National Aerospace University "Kharkiv Aviation Institute", amount of pages 104, amount of tables 25, amount of figures 37, amount of sources of literature 27.

KEYWORDS: hardware key, data protection, establishing a secure connection, medical information system.

PURPOSE OF THE RESEARCH: providing the possibility of establishing a secure connection between the user and the remote server of the medical information system.

OBJECT OF THE RESEARCH: the process of creating a secure connection between a user and a remote medical information system server.

SUBJECT OF THE RESEARCH: methods and technologies for establishing a secure connection with a remote server of the medical information system.

TASKS: to analyze the features of ensuring information protection in medical information systems; analyze existing solutions for a secure connection between the user and the remote server; design scenarios of user interaction with the information protection application; develop an application database; design the application architecture; develop a hardware key to protect the connection with the medical information system; describe the main modes of operation of the application.

METHODS OF THE RESEARCH: information technologies and methods of developing applications and protecting connections for the Windows OS, methods of developing web applications.

RESULTS: a hardware key that increases the reliability of the secure connection between the user and the remote medical information system server is created.

ЗМІСТ

ВСТУП.....	8
1. АНАЛІЗ ІСНУЮЧИХ ПІДХОДІВ І ІНСТРУМЕНТАЛЬНИХ РІШЕНЬ ЗАХИСТУ ІНФОРМАЦІЇ В МЕДИЧНИХ СИСТЕМАХ.....	10
1.1 Актуальність розробки створення захищеного з'єднання між користувачем та сервером медичної інформаційної системи.....	10
1.2 Огляд існуючих засобів які потребують захищеного доступу.....	11
1.2.1 МІС «Каштан».....	11
1.2.2 Медична система «Helsi».....	13
1.2.3 МІС Облік медичних кадрів України та пацієнтів.....	15
1.2.4 Система електронного документообігу Fossdoc.....	17
1.3 Аналіз інструментальних рішень з захисту інформації.....	17
1.3.1 Перші VPN PPTP.....	17
1.3.2 Fortigate.....	19
1.3.3 Cisco.....	19
1.3.4 Ipsec Internet Key Exchange version 2.....	20
1.3.5 Wireguard.....	21
1.3.6 OpenVPN.....	21
1.4 OpenVPN з точки зору кібербезпеки.....	23
1.5 Висновки щодо розглянутих рішень з встановлення захищеного зв'язку.....	26
Постановка задачі.....	28
2 ПРОЕКТУВАННЯ КЛЮЧА ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В МЕДИЧНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ.....	30
2.1 Моделювання дій користувача.....	30
2.2 Опис бази даних.....	32
2.3 Архітектура застосунку.....	36
2.4 API застосунку.....	37
Висновки за розділом 2.....	38
3 ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ АПАРАТНОГО КЛЮЧА ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В МЕДИЧНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ.....	39
3.1 Стек технологій.....	40
3.1.1 AutoIT.....	41
3.1.2 PHP.....	41
3.1.3 MariaDB.....	41
3.2 Особливості використання OpenVPN на різних операційних системах.....	42

3.3 Ліцензування програм для роботи з Open VPN.....	43
Висновки за розділом 3.....	44
4 ОПИС РОБОТИ ЗАСТОСУНКУ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В МЕДИЧНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ.....	45
4.1 Приклад використання застосунку з боку адміністратора.....	45
4.1.1 Пункт UPLOAD.....	47
4.1.2 Пункт SETUP.....	47
4.1.3 Пункт SERVER.....	48
4.1.4 Пункт KEYS.....	52
4.2 Первинний запуск токена.....	55
4.3 Приклад використання з боку користувача.....	58
Висновки за розділом 4.....	62
5 ЕКОНОМІЧНИЙ РОЗДІЛ.....	63
5.1 Визначення тривалості та розрахунок собівартості виконання проекту (програмний варіант).....	63
5.2 Визначення тривалості та розрахунок собівартості виконання проекту (апаратний варіант).....	69
Висновки за розділом 5.....	73
ВИСНОВКИ.....	74
ПЕРЕЛІК ПОСИЛАНЬ.....	76
ДОДАТОК А Демонстраційний матеріал	78
ДОДАТОК Б Програмний код	89

ВСТУП

Актуальність теми дослідження. В останні роки система надання медичної допомоги населенню набула суттєвих змін. З'явилися спеціалізовані системи, які призначені для автоматизації процесів збору, обробки та зберігання інформації, що стосується всіх етапів лікування пацієнта, починаючи від обстеження і зберігання результатів аналізів, закінчуючи формуванням заключень лікаря ті надання рецептів на ліки тощо. При цьому одним із питань, які постають перед розробниками, є забезпечення захисту інформації в медичній інформаційній системі. Медична інформаційна система (МІС) – це інформаційний медичний комплекс програмних систем управління закладом охорони здоров'я. Комплекс призначений для оперативного аналізу і управління всіма сферами діяльності закладу охорони здоров'я.

Інформація, яка зберігається в програмі лікаря, містить персоніфіковані дані хворих, інформацію щодо захворювань та наданих ліків, обігу хвороби, наданих рецептів та результатів аналізів хворого. Ця інформація є конфіденційною, тому повинна бути надійно захищена.

З початку пандемії коронавірусу було обмежено візити до лікарів та місцевих або обласних лікарняних закладів. Стався перехід системи до роботи в режимі онлайн спочатку лікарів, які мали обстежувати хворих, а потім вже й самих хворих, які вносили дані для замовлення ліків та замовлення віддаленого обстеження. Таким чином, питання надання захищеного доступу до медичних інформаційних систем набуло ще більшої актуальності.

Мета і завдання дослідження. Метою кваліфікаційної роботи є надання можливості встановлення захищеного з'єднання між користувачем та віддаленим сервером медичної інформаційної системи.

Для досягнення поставленої мети необхідно вирішити такі задачі:

- 1) проаналізувати особливості забезпечення захисту інформації в медичних інформаційних системах;
- 2) проаналізувати існуючі рішення для захищеного з'єднання між користувачем та віддаленим сервером;
- 3) спроектувати сценарії взаємодії користувача та застосунку для захисту інформації;
- 4) розробити базу даних застосунку;
- 5) спроектувати архітектуру застосунку;
- 6) розробити апаратний ключ для захисту з'єднання з медичною інформаційною системою;
- 7) описати основні режими роботи застосунку.

Об'єктом дослідження є процес створення захищеного з'єднання між користувачем та віддаленим сервером медичної інформаційної системи.

Предметом дослідження є методи і технології встановлення захищеного з'єднання з віддаленим сервером медичної інформаційної системи.

Практичне застосування отриманих результатів. Розроблено апаратний ключ для створення захищеного з'єднання між користувачем та віддаленим сервером медичної інформаційної системи.

Науково-технічний ефект полягає в підвищенні ступеня автоматизації створення захищеного з'єднання між користувачем та віддаленим сервером медичної інформаційної системи.

Економічний ефект пов'язаний зі зниженням витрат на розробку та обслуговування спеціалізованих систем надання захищеного з'єднання між користувачем та віддаленим сервером медичної інформаційної системи.

Апробація результатів дипломної роботи магістра. Результати кваліфікаційної роботи магістра доповідалися і обговорювалися на 27-му Міжнародному молодіжному форумі «Радіоелектроніка і молодь у XXI столітті», секція «Комп'ютерні системи і мережі управління та обробки даних», 10 – 12 травня 2023 р.

Публікації. По темі кваліфікаційної роботи магістра опубліковано тези в матеріалах конференції.

Структура і обсяг кваліфікаційної роботи магістра. Кваліфікаційна робота магістра складається з вступу, 5 розділів, висновків і додатків. Повний обсяг кваліфікаційної роботи магістра становить 104 сторінок, в тому числі: 37 рисунків по тексту; 25 таблиць по тексту; 2 додатка на 27 сторінках; списку використаної літератури з 27 найменуваннями на 2 сторінках.