

Автор:

Карпенко Андреа Тарасович,
студент 41ПЗ групи

Науковий керівник:

Фещенко Богдан Петрович
старший викладач кафедри комп'ютерної та
програмної інженерії

РОЗРОБКА VPN ЗАСТОСУНКА

Анотація. Мета даної роботи полягає у створенні VPN-застосунка, який буде забезпечувати приватне та безпечне з'єднання користувачів під час перегляду контенту в інтернеті. Додаток підтримує ефективні та стабільні протоколи OpenVPN та WireGuard, щоб забезпечити високий рівень захисту інформації та даних.

Ключові слова: VPN застосунок, протоколи з'єднання (OpenVPN, WireGuard), приватність користувачів, анонімність в інтернеті.

Вступ. Наразі, в сучасному світі захист стає все більш важливішим завданням для кожного. Використання VPN-тунелю дозволяє забезпечити ці потреби шифруючи трафік користувача, роблячи будь-які дані нечитабельними для сторонніх осіб. Це корисно для безпечного доступу до корпоративних мереж, обходу географічних обмежень, конфіденційності користувачів.

Постановка задачі. Завданням є написання програмного забезпечення для підключення до VPN. Дослідження буде включати наступні кроки: 1) підтримка протоколів з'єднання (OpenVPN й WireGuard); 2) розробка простого та зручного інтерфейсу для користувача; 3) авторизація; 4) високий рівень безпеки даних.

Мета роботи. Метою роботи є реалізація VPN застосунка на мові програмування C#, який буде забезпечувати захист даних під час підключення до глобальної мережі.

Основна частина. Основна частина буде включати:

- ✓ Огляд протоколів з'єднання (OpenVPN та WireGuard): ключовий аспект бакалаврської роботи полягав в порівнянні та аналізі цих протоколів. Було проведено огляд основних характеристик притоколів, таких як переваги та недоліки, а також проаналізуємо можливості їх використання в різних сценаріях.
- ✓ Підняття VPN-сервера на VDS (Віртуальний виділений сервер): у цьому розділі розглянуто процес налаштування та розгортання VPN-сервера на віртуальному сервері.
- ✓ Тестування ефективності, функціональності протоколів: у даному розділі проводиться тестування VPN-сервера, а саме швидкість з'єднання, пропускну здатність, навантаження на процесор, затримки (ping) під час використання.
- ✓ Створення інтерфейсу для користувачів: в цьому розділі було описано процес розробки інтерфейсу користувача для комфортного використання, а також функції додатка.
- ✓ Реалізація підключення до VPN-серверу через застосунок: у цьому розділі було описано процес розробки додатка для підключення користувачів до VPN-сервера.

Мовою програмування для розробки VPN застосунку було обрано C#. Дана мова має велику бібліотеку стандартних функцій, що робить розробку більше простішою, ефективнішою та забезпечує надійність роботи програми.

Висновок. Отже, результатом роботи буде створення простого у використанні та ефективного VPN додатка, який забезпечує високий рівень безпеки та приватності користувачів з глобальної мережі. Використання такого додатка допоможе користувачеві залишитися анонімним та захищеним.

Список використаних джерел

1. OpenVPN (server). URL: <https://community.openvpn.net/openvpn/wiki/HOWTO#Startingtheserver> (date of access: 10.04.2024).
2. WireGuard (server). URL: <https://www.wireguard.com/#cryptokey-routing> (date of access: 10.04.2024).