РОЗРОБКА КРИПТОГРАФІЧНОЇ СИСТЕМИ НА C# З ГРАФІЧНИМ ІНТЕРФЕЙСОМ

Удовенко М.А., Мєтєльов В.О.
Національний технічний університет "Харківський політехнічний інститут", м. Харків

Мета роботи полягає у створенні програмного забезпечення для захисту конфіденційної інформації шляхом шифрування та дешифрування даних з використанням сучасних криптографічних алгоритмів, а також розробці зручного графічного інтерфейсу користувача.

У сучасному цифровому світі захист інформації набуває критичного значення. З розвитком технологій та зростанням кіберзагроз забезпечення конфіденційності даних стає пріоритетним завданням. Запропонована криптографічна система поєднує надійність сучасних криптографічних алгоритмів з простотою використання.

Розроблена система інтегрує різні типи криптографічних механізмів, включаючи симетричні та асиметричні алгоритми шифрування, а також криптографічні хеш-функції. Програмне забезпечення реалізоване мовою програмування C# з використанням технології Windows Forms для створення графічного інтерфейсу.

Основними функціональними можливостями системи є: шифрування та дешифрування файлів різних форматів; генерація, збереження та завантаження криптографічних ключів; відображення процесу та результатів криптографічних операцій; обробка помилок. Особлива увага приділена системі управління криптографічними ключами, що забезпечує їх надійне зберігання.

Інтерфейс користувача розроблено з урахуванням принципів ергономіки та інтуїтивної зрозумілості. Це дозволяє користувачам без спеціальних знань у галузі криптографії легко виконувати операції шифрування, забезпечуючи при цьому високий рівень захисту даних. Інтерфейс включає візуальні індикатори процесу та детальні повідомлення про помилки.

Розроблена криптографічна система може бути використана як у навчальних цілях для демонстрації роботи різних криптографічних алгоритмів, так і для практичного захисту конфіденційної інформації. Модульна архітектура забезпечує можливість подальшого розширення функціоналу.

Таким чином, представлена робота не лише розв'язує практичну задачу захисту інформації, але й сприяє підвищенню загального рівня інформаційної безпеки. Подальший розвиток проєкту передбачає оптимізацію продуктивності та розширення набору підтримуваних алгоритмів.