

УДК 004

Кучер А.О.¹, Зайко Т.А.²

¹ студ. гр. КНТ-124м НУ «Запорізька політехніка»

² доц. НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ МАТЕМАТИЧНИХ МОДЕЛЕЙ МЕХАНІЧНИХ ПРИСТРОЇВ ШИФРУВАННЯ ДАНИХ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИМУЛЯЦІЇ

Об'єкт дослідження – процес розробки програмного забезпечення для симуляції роботи механічних пристроїв шифрування даних.

Предмет дослідження – програмні засоби для симуляції роботи механічних пристроїв шифрування даних.

Мета роботи – дослідження та розробка програмного забезпечення для симуляції роботи механічних пристроїв шифрування даних.

Матеріали, методи та технічні засоби: мова програмування Python, середовище розробки Visual Studio Code.

В ході виконання роботи було проаналізовано та досліджено механічні пристрої шифрування даних. Сформульовано функціональні вимоги до програмного забезпечення симуляції моделей механічних пристроїв шифрування даних.

Було розроблено та реалізовано програмний симулятор механічної роторної шифрувальної машини, який відтворює принципи роботи класичних електромеханічних криптографічних пристроїв. У процесі виконання роботи проаналізовано теоретичні основи механічного шифрування, спроектовано архітектуру програмного забезпечення, розроблено графічний інтерфейс користувача та реалізовано основні функціональні модулі симулятора.

Розроблене програмне забезпечення надає можливість налаштування роторів, плагборду та відбивача, виконує коректне крокування роторного механізму, здійснює шифрування введених символів у режимі реального часу та веде журнал результатів роботи. Проведене тестування підтвердило правильність і стабільність функціонування програми, а також її відповідність поставленим вимогам.

Визначено, що механічні пристрої шифрування не лише виконували практичну функцію захисту інформації, а й сприяли формуванню теоретичних основ криптографії. Аналіз принципів їх роботи дозволив сформулювати ключові криптографічні поняття, зокрема роль ключа як параметра безпеки, необхідність оборотності перетворень, значення композиції операцій та залежність криптографічної стійкості системи від складності її математичної структури. Саме досвід використання механічних шифраторів показав, що безпека системи не може ґрунтуватися виключно на секретності її конструкції.

За результатами проведеного аналізу зроблено висновок, що побудова математичних моделей дає змогу перейти від інтуїтивного розуміння процесів шифрування до формального аналізу, що є необхідною умовою для розроблення надійних програмних засобів захисту інформації. Водночас дослідження механічних шифрувальних пристроїв з позицій сучасної математики дозволяє глибше усвідомити еволюцію криптографічних методів та закономірності їх розвитку.

Тому актуальною є розробка програмного забезпечення для симуляції роботи механічних пристроїв шифрування даних.

Сформульовано функціональні вимоги до програмного забезпечення симулятора роботи пристрою шифрування даних.

Для реалізації програмного забезпечення симуляції роботи пристрою шифрування даних обрано мову програмування Python. Використання Python дозволяє ефективно реалізувати алгоритми симуляції, забезпечити наочність роботи програмного забезпечення та спростити подальше розширення функціональних можливостей системи.

Для реалізації програмного забезпечення обрано середовище розробки Visual Studio Code, що обґрунтовано його кросплатформенністю, гнучкістю налаштувань та широкими можливостями розширення. Підтримка мови Python, інтеграція з системами контролю версій, налагоджувачами та зовнішніми інструментами аналізу коду роблять Visual Studio Code зручним і ефективним середовищем для розробки прикладного програмного забезпечення дослідницького та навчального призначення.

Новизна роботи полягає у тому, що створено програмний симулятор механічної шифрувальної машини з розширеним навчальним функціоналом, який поєднує точне відтворення логіки роботи роторного механізму з наочним графічним інтерфейсом і можливістю детального аналізу процесу шифрування. На відміну від існуючих реалізацій, розроблений симулятор орієнтований не лише на отримання результату шифрування, а й на демонстрацію внутрішніх етапів роботи шифрувального пристрою.

Практичне значення роботи полягає у можливості використання розробленого програмного забезпечення в освітньому процесі для вивчення

основ криптології, історичних методів шифрування та принципів побудови симетричних криптографічних систем.

Визначено, що основними класами симулятора механічної шифрувальної машини є: SimulatorController, CipherDevice, JeffersonCylinder, RotorMachine, Клас Rotor, TextIO, Alphabet, FrequencyAnalyzer, ReportGenerator, ProjectStorage та інші.

Описано функціонування програмного забезпечення симулятора механічної шифрувальної машини.

Описано особливості реалізації програмного забезпечення симуляції механічного пристрою шифрування даних.

Виконано проектування інтерфейсу симулятора механічної шифрувальної машини.

Виконано тестування розробленого програмного забезпечення симуляції механічної роторної шифрувальної машини. Результати тестування програмного забезпечення показали, що розроблена програма дозволяє наочно відтворювати роботу класичних механічних шифрувальних пристроїв, змінювати конфігурацію шифрувального механізму, аналізувати результати шифрування.

Галузь використання – навчальні, дослідницькі та демонстраційні цілі.