РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ШИФРУВАННЯ ПОВІДОМЛЕНЬ З ВИКОРИСТАННЯМ ВИПАДКОВОЇ ПОСЛІДОВНОСТІ

канд. техн. наук, проф. О.М. Рисований, студ. С.С. Соболенко, Національний технічний університет "Харківський політехнічний інститут", м. Харків

Актуальність теми шифрування інформації збільшується зі зростанням числа кібератак, розвитком технологій, таких як Інтернет речей (IoT), витоків персональних даних людей, використанням хмарних сервісів та квантових обчислень. Шифрування стає не тільки бажаним, а необхідним. Крім того, законодавчі ініціативи на міжнародному рівні вимагають використання сучасних методів захисту даних, зокрема шифрування, для забезпечення відповідності нормам.

Особливої актуальності шифрування набуває в умовах гібридних загроз, кібервійн та інформаційних протистоянь. Захист комунікацій, державних баз даних, військових систем і критично важливої інфраструктури без ефективного шифрування стає неможливим [1 – 3].

Метою роботи є розробка програмного продукту для отримання випадкової послідовності, шифруванню файлів та їх дешифруванню. Основою отримання випадкової послідовності є кількість мілісекунд, що пройшли з моменту запуску системи, яку повертає API-функція GetTickCount, та дорівнює до 49,7 днів.

Практично доведено, що отримана випадкова послідовність відповідає зазначеним вимогам.

Список літератури: **1**. Рисований О.М., Ігнатьєв К.І., Рибалка Р.В., Рудаковський Д.Р. Механізм шифрування повідомлень з максимальною довжиною // Інформатика, управління та штучний інтелект. Тези одинадцятої міжнародної науково-технічної конференції. – Харків: НТУ "ХПІ", 2024. – 176 с. – С.127. **2.** Рисований О.М., Ігнатьєв К.І., Рибалка Р.В., Рудаковський Д.Р. Вибір багаточленів з максимальним періодом генерації станів // Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: тези доповідей XXXII міжнародної науково-практичної конференції MicroCAD-2024, 22-25 травня 2024 р. / за ред. проф. Сокола Є.І. – Харків: НТУ "ХПІ". – С. 1421. **3.** Рисований О.М. Криптостійний генератор псевдовипадкової наслідності з використанням майстер-ключа // Проблеми інформатики та моделювання (ПІМ-2024). Тези двадцять четвертої міжнародної науково-технічної конференції. – Харків: НТУ "ХПІ", 2024. – С.120.