**АНОТАЦІЯ**

РОЗРОБКА СИСТЕМИ ШИФРУВАННЯ ПОВІДОМЛЕНЬ ВЕЛИКИХ РОЗМІРІВ

Автор роботи: Попович Ярослав Васильович;

Харківське територіальне відділення МАН України;

Харківський навчально-виховний комплекс №45 «Академічна гімназія»

Харківської міської ради Харківської області; 10 клас; м. Харків

Науковий керівник: Руккас Кирило Маркович,

професор кафедри теоретичної та прикладної інформатики механіко-математичного факультету Харківського національного університету

імені В. Н. Каразіна, доктор технічних наук, доцент

Нині активний розвиток і поява нових інформаційних технологій постійно вимагають підвищення ефективності та рівня захисту інформації. Забезпечити додатковий захист даних дозволяє шифрування. Саме тому ця тема є актуальною.

Мета дослідження - знаходження оптимального алгоритму для шифрування повідомлень великого розміру на будь-якому обладнані.

Об'єкт дослідження - процес швидкого шифрування даних великого обсягу.

Предмет дослідження - алгоритми шифрування даних.

Методи дослідження: вивчення досвіду фахівців, аналіз та порівняння.

Для досягнення мети були виконані такі завдання: проаналізовані існуючі алгоритми шифрування; був розроблений новий алгоритм шифрування даних мовою С++ і python; був розроблений консольний чат мовою python 3.7.4 за допомогою бібліотеки ; створені тести; порахована асимптотика роботи алгоритмів та були протестовані алгоритми в реальних умовах (на прикладі розробленого чату); проведений порівняльний аналіз роботи алгоритмів шифрування за часом, пам'яттю та кількістю потрібних ключів.

В результаті було визначено, що розроблений алгоритм краще всіх інших працює на великих рядках, а на малих краще себе показує шифр DES.

На практиці ця робота може бути використана для безпечної відправки повідомлень великого розміру на обладнанні будь-якої потужності.

Ключові слова: шифрування, алгоритм, великі повідомлення, безпека, чат.