УДК 519.7

# А. ТЬЮРІНГ І ШИФРУВАЛЬНА МАШИНА «ЕНІГМА»

Студ. Ю.А. Тимченко, гр. БОА-1-17
Науковий керівник доц. О. Л. Блохін
Київський національний університет технологій та дизайну

***Мета*** дослідження - аналіз роботи та сфера використання шифрувальної машини «Енігма».

***Завдання:***

- вияснити мету створення даного винаходу;
- дослідити будову та механізм роботи шифрувальної машини;
- розглянути внесок А. Тьюрінга в розвиток сучасних технологій.

***Об'єкт дослідження*** – кодування інформації в роки Другої світової війни.

***Предметом дослідження*** – є шифрувальна машина «Енігма»

***Методи дослідження***: порівняльно-історичний метод, системний аналіз та ін.

***Наукова новизна.*** Робота над «Енігмою» призвела до появи нових винаходів в напрямку шифрування і розкодовування інформації, а також було створено перший в світі комп'ютер.

***Практичне значення отриманих результатів***. Матеріали дослідження можуть бути використані для підготовки рефератів на семінарських та практичних заняттях та в подальших дослідженнях теорії кодування.

***Результати дослідження:***

У XIX сторіччі людство почало все інтенсивніше використовувати засоби комунікації, а разом з цим виникла необхідність автоматизувати процес шифрування. З винаходом телеграфу виникла необхідність шифрувати і його. Особливо , шифрування було потрібним у роки війни.

У 1917 році голландець Кох запатентував електричний роторний пристрій для захисту комерційної інформації. У 1918 році німець Шербіус купив цей патент, допрацював його і побудував шифрувальну машину, яка отримала назву «Енігма».

Завдяки відносній простоті використання та важкості таких шифрів, система «Енігма» була вибрана німецьким урядом для шифрування більшої частини військових донесень в роки Другої світової війни. Саме через це розшифрування кодів «Енігми» стала абсолютним пріоритетом для правлячих кіл країн, що воювали з Німеччиною.

Історія розшифровки кода «Енігми» -це захоплююча епопея з участю відділів розвідки Польщі, Великобританії, а також ідеального математика Алана Тьюрінга, людини, яку вважають батьком сучасної обчислювальної техніки.

Як і інші роторні машини «Енігма» складалася з комбінації механічних та електричних підсистем. Механічна частина включала в себе клавіатуру, набір обертових дисків- роторів, які були розташовані вздовж валу і прилягали до нього, та ступеневої механізму, що рухає один або кілька роторів при кожному натисканні на клавішу. Електрична частина, в свою чергу, складалася з електричної схеми, що з'єднує між собою клавіатуру, комутаційну панель, лампочки і ротори (для з'єднання роторів використовувалися ковзні контакти).

Математичний опис роботи шифрувальної машини «Енігма»

Перетворення «Енігми» для кожної літери може бути визначено математично як результат ˈперестановок. Розглянемо трьохроторную армійську модель.

Припустимо, що «P» позначає комутаційну панель, «U» позначає відбивач, а «L», «M», «R» позначають дії лівих, середніх і правих роторів відповідно. Тоді шифрування «E» може бути виражено як

$$E=PRMLUL^{-1}M^{-1}R^{-1}P^{-1}$$

Після кожного натискання клавіш ротор рухається, змінюючи трансформацію. Наприклад, якщо правий ротор «R» провертається на і позицій, відбувається трансформація : $\rho^{i}R\rho^{-i}$, де , де ρ - циклічна перестановка, що проходить від «A» до «B», від «B» до «C», і так далі. Таким же чином, середній і лівий ротор можуть бути позначені як j і k обертань «M» і «L». Функція шифрування в цьому випадку може бути відображена в такий спосіб :

$$E=P(\rho^{i}R\rho^{-i})(\rho^{i}M\rho^{-j})(\rho^{k}L\rho^{-k})U(\rho^{k}L^{-1}\rho^{-k})(\rho^{j}M^{-1}\rho^{-j})(\rho^{i}R^{-1}\rho^{-i})P^{-1}$$

Під час Другої світової війни Тьюринг працював в Блетчлі-парку – британському криптографічному центрі, де очолював одну з п'яти груп, Hut 8, займалися в рамках проекту «Ультра» розшифровкою закодованих німецької шифрувальної машиною «Енігма» повідомлень крігсмаріне і люфтваффе. Внесок Тюрінга у роботи з криптографічного аналізу алгоритму, реалізованого в «Энигме», ґрунтувався на більш ранньому крипто аналізу попередніх версій шифрувальної машини, виконаних в 1938 році польським крипто аналітиком Маріаном Реевским.

Напружена робота шифрувальників під керівництвом Тюрінга увінчалася успіхом: було створено пристрій, здатний розшифрувати сигнали «Енігми». Крім усіляких математичних хитрощів, у якості підказок використовувалися одні і ті ж стереотипні фрази, за допомогою яких спілкувалися німці, а також будь-які повторюються тексти.

***Висновки***

Хто володіє інформацією – володіє Світом. Цю істину двісті років тому сформулював англійський банкір Натан Ротшильд після поразки Наполеона в битві при Ватерлоо. Захист інформації , як і в давні часи, так і сьогодні, є важливим чинником під час війни. Для цього було створено велику кількість кодів, шифрів і шифрувальних механізмів. В разі витоку або перехвату інформації зі сторони суперника, дана інформація буде зашифрованою. Звичайно, з плином часу, цю інформацію могли розшифрувати, але , мабуть, вона вже не буде актуальною.

Шифрувальна машина «Енігма» - це дуже важливий винахід, розшифрування інформації якої було метою, можна сказати навіть необхідністю, багатьох країн світу. Недарма А.Тьюрінга вважають батьком сучасної обчислювальної техніки. Завдяки ньому з'явився перший в світі комп'ютер ,який, до речі, грав велику роль як і у воєнні роки, так і в наш час.

## ЛІТЕРАТУРА

1. Сингх С. Книга шифров .Тайная история шифров и их расшифровки. — Астрель, 2007
2. Жельников В. Криптография от папируса до компьютера. — ABF, 1996.
3. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии. — Мир, 2007.
4. Смарт Н. Криптографія. Серія «Світ програмування». - Техносфера, 2005. 528 с.