УДК 003.26

А. О. Михальчук
аспірант кафедри культурології
Східноєвропейського національного університету імені Лесі Українки

СИСТЕМИ КОДУВАННЯ ІНФОРМАЦІЇ В АНТИЧНУ ДОБУ (ФІЛОСОФСЬКО-СЕМІОТИЧНИЙ АСПЕКТ)

Код є одним з основних способів збереження інформації. З розвитком філософії як науки та зародження семіотики у добу античності, символ став одним із ключів до розуміння природи.

В історичних документах стародавніх цивілізацій Індії, Єгипту, Месопотамії та Китаю є відомості про цілі системи і способи складання шифрованого письма, що утворювали своєрідні гектограми, гексограми, малюнки, геометричні фігури, поєднання алфавітів різних народів, своєрідних предметів, котрі створювалися таким чином, щоб непосвячені не здогадались про значення «тайнопису». Метою створення коду був запис інформації у хаотичному вигляді, і лише людина, яка знала ключ, мала змогу прочитати написане. Чим простіше написаний код (без необхідних ключів), тим складніше його розгадати.

Поняття «код» набуло великої популярності в епоху античності та зумовлювалося пошуком нових систем кодування серед провідних цивілізацій «Стародавнього Світу». Саймон Зінгх говорив: «Протягом багатьох століть королі, королеви й генерали покладалися на ефективність зв'язку для того, щоб управляти країнами та командувати своїми військами. У той же час, вони всі були обізнані про наслідки своїх повідомлень, якщо ті потраплять у ворожі руки, відкриваючи дорогоцінні секрети конкуруючих націй та життєво важливу інформацію для протилежних сил. Це була загроза ворожих перехоплень, які мотивували зародження кодів та шифрів як способу маскування повідомлення так, щоб тільки «посвячені» змогли прочитати його зміст» [11]. Ось якою важливою і необхідною може виявитись інформація.

До сучасників, які займаються дослідженням історичної періодизації криптографії, належать John Chadwick, Priya Hemenway, E. Edvard Hulme, Kennet Johnson, David Kahn, Richard Mollin, Kenneth Rossen, Simon Singh, Michael Smith та багато інших дослідників сучасності.

Метою дослідження є характеристика становлення та розвиток систем кодування в античну добу, філософсько-семіотичний аспект.

Завдання: пояснити значення коду та порівняти вплив різних систем кодування на розвиток культур Сходу (Стародавнього Китаю) та Заходу (Стародавньої Греції та Риму).

Різні цивілізації стрімко розвивались та занепадали в епоху античності. Особливістю кожної культури було становлення їх величі на різних територіях Сходу (Стародавнього Світу), а також цінності, які цивілізації набували за допомогою знань та віровчень. Знання, які збагачувались від покоління до покоління до III тисячоліття до н.е. передавались виключно словесно. З появою письма новою проблемою стало перенесення відповідної інформації на пергамент. З початком розвитку цивілізацій Єгипту та Китаю було започатковано запис інформації за допомогою ієрогліфічного, демотичного письма або клинописних гачків.

Із записів Джона Чедвіка: «Криптографія сприяла розвитку нової зброї. Сьогодні код може бути теоретично розшифрованим, якщо наведено достатню кількість прикладів закодованих текстів. Єдиним способом, за допомогою якого можна розшифрувати код, є забезпечення безперервної зміни у системі кодування, щоб дешифрувати знаки без ключів було практично не можливо. Основними принципами дешифрування є аналіз та індексація закодованих текстів, так, щоб основні шаблони і закономірності могли бути виявлені. Певна група знаків у кодованому тексті має конкретну функцію і на розуміння його може вплинути будь-яка деталь» [7, с. 40]. Джон Чедвік – англійський математик, який вперше дешифрував код мінойського періоду Стародавньої Греції III-II тис. до н.е. (грецьких міст Кноссу, Мікен та Кіпру) у 1950-х рр. XX ст. Підхід, який застосував математик Джон Чедвік, тісно переплітається з семіотичними концепціями Ф. де Соссюра та Ч. Пірса.

Набуття коду, як елементу демотичного письма дослідив античний філософ та вчений **Абу Юсуф Якуб ібн Ісхак ібн ас Сабах ібн Умран ібн Ісмаіл аль Кінді.** Учений займався дешифруванням даних різних рукописів античності, а також окремих філософських трактатів. Його найвідоміший трактат «Рукопис із дешифрування криптографічного письма» IX ст. до н.е. був знайдений у 1987 році в оттоманському архіві Сулайманія у Стамбулі. Абу аль Кінді був автором понад 300 книг з медицини, астрономії, математики, лінгвістики, музики та інших дисциплін.

Трактат «Рукопис із дешифрування криптографічного письма» містив у собі низку способів дешифрування криптографічного письма шумеро-акадського періоду (I пол. III тис. до н.е.), а також тлумачення окремих типів ієрогліфічного письма та періодику підбору слів за допомогою математичних обрахунків і підставлення їх до алфавіту [2].

Уперше в епоху античності із набуттям писемності почали формуватися різні релігійні групи людей для трактування священних текстів і шифрування їхнього змісту від непосвячених. Кожна із груп мала відповідні рекомендації для секретарів *«Адаб аль Куттаб»* (до X ст н.е.). Ці рекомендації описували низку правил для запису зібрань зашифрованим письмом, значення якого знали лише лідери групи.

Також були відповідні касти людей, які прагнули здобути знання попередніх цивілізацій різними можливими та неможливими способами. Наприклад, династія халіфів Аббасидів мала високе становище у суспільстві. Система низьких податків, розвиток комерційної діяльності та торговельних відносин забезпечили процвітання на Близькому Сході серед мусульман, а також вельми суворі закони щодо запобігання корупції забезпечили безпеку своїх громадян – і все це виливалось у відповідних правилах, які записувались виключно зашифрованим текстом.

Наповнення «коду» сакральним змістом детально описав Арістотель Стагіріт у своїй праці «Органон». Одна із найбільш оригінальних та детально вивчених семіотичних ідей «коду» та «знаку» описується у «Першій аналітиці» Арістотеля – визначення ентимеми, як силогізму поняття «знаку». Ось як це пояснює Арістотель в останньому розділі «Перша Аналітика»: «Якщо визнати <…>, що така властивість має свій відповідний знак, і якщо визнаємо, що кожному роду живих істот присутня особлива властивість та відповідний знак, то ми у змозі розпізнати природу цих речей. А саме, якщо будь-якому роду… притаманна відмінна властивість, як, наприклад, левам – сміливість, то необхідно, щоб був якийсь його власний «знак», його власна сутність… Одна властивість… має один знак» [1, с. 253-254]. Знак – це «ідеальна пропорція», яка пояснює тонку грань предмета і дає нове означення даного предмета.

Активно до розвитку криптографії залучилися території різних провінцій Китаю; Вавілонії та Акаду, де активно застосовувався одноалфавітний шифр заміни; Шумеру, де поєдналися шифрування не тільки алфавіту, а й різноманітних малюнків; Єгипту, де активно застосовувалося шифрування письма за допомогою малюнків із книг «Життя та Смерті», а також іменування божеств у папірусах; Карфагену, де зашифровувалась інформація лише у військових кампаніях і тільки на зброї. Все це дало початок зародження криптографії в античній Європі.

В одній із хронік Геродота – «батька історії», одним із найвідоміших переломних моментів став завойовницький наступ Ксеркса, царя царів, лідера персів на Грецію у 480 році до н.е. Геродот розглядав цей конфлікт як протистояння між свободою і рабством, між незалежними грецькими державами та войовничою Персією. Мистецтво «секретного листа» врятувало Грецію від підкорення.

«Знак» у період античності не тільки застосовувався як спосіб передачі інформації, а й дослідження знака у природі, у людині. Розуміння сенсу життя теж використовує власні способи кодування, які людина мусить розшифрувати впродовж свого життя. Одним із таких понять був символ *«Ф»* (φ-фи) – не тільки 21 буква грецького алфавіту, а й «золотий перетин» (золота пропорція, розподілу у крайньому та середньому відношенні, гармонійного розподілу) – сакрального співвідношення двох величин a та b. Символ *«Ф»* названий у честь давньогрецького архітектора Фідія. Ось як описує Priya Hemenway символ «золотого перетину *«Ф»:* «Люди у минулому намагались зрозуміти питання про те, хто ми і що ми. Для цього вони розробили декілька способів, щоб висловлювати екзистенційні істини за допомогою пропорцій. За античних часів було багато дивовижного, коли цифри об'єднують у собі містичні відносини та божественні співзвуччя, що були частиною мови розвиваючої математики. Це була мова реальних і символічних додатків, що мали незвичну здатність розшифровувати таємниці. Як мова, математика лежить десь між світами, яка може бути перекладена на іншу мову, і трактуватись як мистецтво – таємниче, гармонійне, що стає частковим рішенням практичних головоломок філософської думки» [7].

Уперше відомий текст, що містить компоненти криптографії бере свій початок в єгипетському місті Менет Хуфу на могилі дворянина Кнумхотеп II майже 4000 років тому. Приблизно у 1900 р до н.е. писар Кнумхотепа описав усе життя свого господаря в його могилі. Коли він малював ієрогліфами, використовував ряд незвичайних символів, щоб приховати зміст написів. Цей метод шифрування є яскравим прикладом першого коду підставляння, який, як будь-яка система шифру, замінює один символ на інший.

Під час розквіту єгипетської культури ієрогліфічне шифрування стало більш поширеним явищем. Цей метод шифрування було відносно легко дешифрувати для тих, хто міг читати й писати стародавньою єгипетською мовою. І це зумовило створення більш складних шифрів для безпеки даних.

Приблизно у 500 р до н.е. спартанці розробили пристрій під назвою зашифрованих повідомлень *„Scytale"*. Пристрій складався із циліндра потрібної довжини і повідомлення записувалися на пергаменті. Після того, як повідомлення було написано, пергамент розрізався на смужки та ставав не читабельним. Для того, щоб отримати повідомлення, необхідно було мати ідентичної довжини циліндр. Лише тоді, посвячена людина змогла б дешифрувати послання. *Scytale* був одним із засекречених способів передачі інформації у Стародавній Греції та довгий час був незламним.

Атбаш – це простий код підставляння букв алфавіту івриту. Приклади використання даного коду можна зустріти у священних юдейських текстах, у тому числі у книзі пророка Єремії (VI століття до н.е.), де активно застосувався простий метод шифрування атбаш.

Пізніше, у добу середньовіччя, атбаш активно застосовувався в окультних ученнях, які поєднували різні діалекти івриту, арамейської, санскриту та інших мертвих мов.

Використання способів кодування у військових кампаніях набуло популярності при правлінні римського імператора – Юлія Цезаря. Цезар, будучи командиром римської армії, вирішив проблему безпечного спілкування зі своїми військами без посвячення в інформацію великої кількості людей. Проблема полягала у тому, що посланці секретних військових повідомлень могли бути ворогами і не виконати безпосередньо відданого наказу. Для цього Цезар розробив метод підміни шифру, в якому він замінював кожну літеру алфавіту. Це дало римській армії величезну перевагу під час військових кампаній. Сьогодні цей шифр активно використовується при кодуванні комп'ютерних повідомлень за допомогою систем передачі даних зі змінним порядком розташування букв алфавіту.

Відповідно до наведених вище основних, знайдених під час розкопок фрагментів кодів зашифрованого письма, є можливість порівняти шифри різних цивілізацій. Одна із цитат Саймона Зінгха про «код»: «шифрувати і дешифрувати секретні повідомлення було священним заняттям. Проте коди, як і шифри, почали споріднюватись і набувати сенсу незалежно від їх семантичного або мовного значення. Упродовж історії термін «код» став віддаленим від поняття «шифр» і набув свого значення саме в епоху античності, довівши свою значущість і практичну користь для людей різних верств населення» [9].

З розвитком коду людство почало вивчати іншу сторону природи, а саме – людину. Код, як його розуміє Умберто Еко – це невіддільна частина душі людини, яка шукає себе у суспільстві. Зародження семіотики дозволило не тільки ширше подивитись на світ, але і збагатити своє розуміння свого місця у суспільстві.

Найбільшим відкриттям у розшифруванні писемності античності став «Розетський камінь». На початку другого століття до нашої ери, витесаний каменярами, був створений кам'яний блок у Єгипті, який набув форми воріт із зображенням усіх єгипетських ієрогліфів відомих династій. Це було найграндіозніше відкриття століття. У серпні 1779 р. недалеко від міста, відомого європейцям як *Rosetta,* яке знаходиться недалеко від культурної столиці Єгипту – Александрії, був знайдений кам'яний блок. Камінь був неправильної форми із чорного базальту з відломленими (відсутніми) шматками.

На камені зображено три різних системи письма: грецькі літери, ієрогліфи й демотичне письмо, яке є прообразом ієрогліфічного письма. Таким чином, це дало можливість розшифрувати єгипетське ієрогліфічне письмо у масштабі, якого не бачили раніше. Вважається, що написи були зроблені жерцями Мемфіса у дев'ятому році правління Птолемея V Єпіфана (205–180 рр. до н.е.) на честь процвітання та продовження царювання. Щоб відсвяткувати, жерці зробили золоті статуї фараона в Єгипетських храмах, а також копії ухвал. Цей указ був розрізаний на базальтові плити на три частини і розміщений у храмах біля статуй.

Отже, припущенням учених було те, що ці три шматки були з того ж відкритого тексту, так би мовити, коду життя фараона. Багато талановитих дослідників було залучено до розшифрування текстів «Розетського каменя». Сьогодні вважається, що на камені зображено «мовне дерево існування життя на Землі», що є своєрідним кодом, який потрібно ще розшифрувати.

Висновки дослідження. У добу античності системи кодування набули багатьох значень. Створення різноманітних шифрів не лише доповнили арсенал військового потенціалу цивілізацій, а й стали ключем до розуміння філософії людського мислення. Писемність почала зароджуватись у добу античності, яка суттєво посприяла розвитку коду та систем кодування. Створення системи запису знаків стало основним етапом у розвитку коду, що у свою чергу, розширило розуміння важливості інформації для людей доби античності.

Література

1. Быков Ф. С. Зарождение политической и философской мысли в Китае / Ф. С. Быков. – М., 1966. – С. 155.

2. Зингх Саймон. Книга шифров. Тайная история шифров и их расшифровки / Зингх Саймон. – М. : АСТ : Астрель, 2009. – 447 с.

3. Кеплер И. О шестиугольных снежинках / И. Кеплер. – М., 1982. – С. 93.

4. Перевод Сратановского Г.А. по изд.: Геродот. История в девяти книгах. – Л., 1972.

5. Спирин В. С. Построение древнекитайских текстов. – М., 1976. – С. 50.
6. Dlels H. Die Pragmente der Vorsokratiker / H. Dlels, Kranz W. – Berlin,1934
7. Hemenway Priya. The Secret Code. The mysterious formula that rules art, nature and science / Priya Hemenway. – K ln : Evergreen, 2008. – 203p.
8. F.Edvard Hulme. Cryptography, Principles and Practice of Cipher Writning / F. Edvard Hulme. – London, 2013. – 198 p.
9. Kahn D. The Code breakers / D. Kahn. – New York, 1973. – 473 p.
10. Richard A. Mollin. The Guide to Secrecy from ancient to modern times / Richard A. Mollin. – NY. : Chapman & Hall, 2005. – 700 p.
11. Singh Simon. The Code book: Science secrecy cryptography / Singh Simon. – London : Anchor, 1999. – 424p.
12. Keiji Yamada. The formation of the Huang-tiHeiching / Keiji Yamada // Acta Asiatica, Bulletin of the Institute of Eastern Culture. – Tokyo, 1979, – P. 67.

Анотація

Михальчук А. О. **Системи кодування інформації в античну добу (філософсько-семіотичний аспект).** – Стаття.

У статті розглядається філософсько-семіотичний аспект становлення та розвитку систем кодування інформації в античну добу. Елементами наукової новизни статті є, по-перше, обґрунтування концептуального значення термінів «знак» та «код» у системі кодування, по-друге, дослідження процесів створення кодів у добу античності, по-третє, практичне перенесення систем кодування від усного до писемного на основі різних лінгвістичних груп.

Становлення різних систем кодування у добу античності об'єднало у собі підвиди семіотики: етносеміотику, лінгвосеміотику та семіологію. Писемність почала зароджуватись у добу античності, яка суттєво посприяло розвитку коду. Створення систем запису знаків стало основним етапом у розвитку коду, що, у свою чергу, розширило розуміння важливості інформації для людей доби античності.

Ключові слова: Ф, код, писемність, цивілізація, криптографія, тайнопис, шифрувальний пристрій, гектограма, філософія античності.

Аннотация

Михальчук А. О. **Системы кодирования информации в античные времена (философско-семиотический аспект).** – Статья.

В статье рассматривается философско-семиотический аспект становления и развития систем кодирования в античные времена. Элементами научной новизны являются, во-первых, обоснование концептуального значения терминов «знак» и «код» в системе кодирования, во-вторых, исследования процессов создания кодов в античности, в-третьих, практическое значение переноса систем кодирования от устного к письменному на основе различных лингвистических групп. Становление различных систем кодирования в эпоху античности объединило в себе подвиды семиотики: этносемиотику, лингвосемиотику и семиологию. Письменность начала зарождаться в эпоху античности, которая существенно способствовала развитию кода. Создание системы записи знаков стало основным этапом в развитии кода, в свою очередь, расширило понимание важности информации для людей эпохи античности.

Ключевые слова: Ф, код, письменность, цивилизация, криптография, тайнопись, шифровальный устройство, гектограмма, философия античности.

Summary

Mykhalchuk A. O. **Information coding systems in ancient (philosophical and semiotic aspects).** – Article.

The article analyzes the formation and development of coding in ancient in philosophical and semiotic aspects. The elements of scientific novelty is, first of all, study the conceptual meaning of the terms "sign" and "code" in the coding system, secondly, the study of the processes of creating code in ancient, thirdly, practical transfer coding systems from oral to written based in different more linguistic groups. The formation of different coding systems in ancient united in a subspecies of semiotics: ethno-semiotics, lingvo-semiotics and semiology. The writing almostly began to emerge in the ancient, which significantly contributed the development of the code. Creating a system of recording marks was a major step in the development of the code, which in turn increased the awareness of the importance of information for those days of antiquity.

Key words: Ф, code writing, civilization, cryptography, cryptography, encryption device hektohrams philosophy of antiquity.