УДК 101.8

Михальчук А. О.,
аспірант кафедри культурології,
Східноєвропейський національний університет
ім. Лесі Українки (Україна, Луцьк), Potter15@list.ru

Проблема криптографії: семіотичний аспект

Досліджуються особливості криптографічного коду, судження поняття «код», та його значення. Експлікуються філософські терміни «символ» та «знак». Обґрунтовується, що код є невід'ємним елементом криптології, який лежить у контексті семіотичного підходу, та зводиться до логічного осмислення всієї різноманітності культурних цінностей. Знак та символ уособлює в собі поєднання різних сфер медіа культурного простору та метафізичних узагальнень математики, фізики, астрономії та архітектури. Однак існує й більш специфічний сенс криптографії: її методи використовувалися для встановлення зв'язку між земним світом і Світом Небесним.

Ключові слова: *знак, символ, код, криптографія, семіотика, шифр, магія.*

Поняття «криптографія» – це, так би мовити, універсальна мова захисту, яку людство використовує протягом багатьох віків. Шифрування – єдиний спосіб захистити наше приватне життя і гарантувати успішне функціонування електронного ринку. Мистецтво секретного зв'язку, відоме як криптографія, дасть вам замки й ключі від інформаційного століття.

За період вікової історії відбулося досить багато подій, які дали поштовх до заснування криптографії як науки. Аналітичне тлумачення літер завжди було першоджерелом для існування думки. Серед сучасних дослідників виокремилися такі світові науковці, як E. Edvard Hulme, Kennet Johnson, David Kahn, Otto Ran, Simon Singh, Michael Smith, Жиль де Поп, та вітчизняні: Л. С. Павлюк, а також багато інших провідних учених сучасності.

Мета статті: аналіз семіотичного аспекту криптографії динаміки та її використання у житті суспільства.

Поставлена мета передбачає виконання таких завдань: експлікувати поняття «криптографія»; розкрити зміст поняття «код»; проаналізувати співвідношення між філософськими термінами «символ» та «знак», пояснити значення коду як семіотичної категорії.

Історія захисту інформації починається десь у той час, коли люди почали спілкуватися за допомогою писемності. І це зумовило потребу її захисту від «непосвячених». Відомо, що в Стародавній Греції голову раба голили, писали на його голові, чекали, коли волосся знову виросте, після чого відправляли з дорученням до адресата. Потреба переховування знань від «непосвячених» сприяло розвитку ідей захисту інформації коду та створення систем кодування. «Коди – це спосіб поєднання знаків, правила, які впорядковують їх рух і взаємозв'язок» [1, с. 25].

Вперше поняття «криптографія» (від грецького *kryptos* – прихований і *graphein* – писати) з'явилось ще в давнину, разом із писемністю. Майже чотири тисячі років тому в давньоєгипетському місті Менет–Хуфу на березі Нілу один досвідчений переписувач намалював ієрогліфи, що розповіли історію життя його пана. Зробивши це, він став родоначальником документально зафіксованої історії криптографії [4, с. 5]. Його система не є тайнописом в тому вигляді, в якому вона відома сучасному світу. Для засекречення свого напису він не використав жодного повноцінного шифру. Цей напис, вирізаний ним приблизно в 1900 р. до нашої ери на гробниці знатної людини на ім'я Хнумхотеп, лише в окремих місцях складається з незвичайних ієрогліфічних символів замість більш звичних ієрогліфів. Таким чином, переписувач застосовував не тайнопис, він, безперечно, скористався одним із істотних елементів шифрування умисним перетворенням письмових символів. Це найдавніший відомий нам текст, який зазнав таких змін.

«Символ – «емотивований знак», репрезентація об'єкта на основі матеріальної форми, яка є довільною щодо зображуваного. Знак–символ не зберігає прямого предметного зв'язку із об'єктом чи концептом, який репрезентує, і тому слугує узагальненню, відкриває логічний простір для метафізики у пірсеанському сенсі – думок про думки, мислення про мислення. Символи – це найчисленніша група знаків: цифри, власні імена, назви предметів і понять. Їх значення вважають результатом суспільної згоди, конвенції» [1, с. 9]. Ось так розкриває значення цього терміну Л. Павлюк, наголошуючи на специфічному розумінні символу в семіотичному контексті.

Перш за все, символ – це умовне позначення будь–якого предмета, поняття або явища, що зближує його із поняттям «знак». Символ є одним із ключових понять у філософії, філології, естетиці, математиці, оскільки без нього не можливо побудувати ні теорію мови, ні теорію пізнання, ні математичного доведення. У кожній науці поняття символу розуміється «по–своєму», зокрема семіотика розглядає символ як різновид знаків.

У концепції Ч. Пірса знаковий принцип проголошено основним логічним принципом будь–якого культурного самовираження. Умовність щодо реальності функції елементів репрезентативного ряду дозволяє сягати речей, віддалених у часі і просторі. Фізіологічний апарат людини пристосований до опрацювання знакової інформації – слів, цифр, символьних позначень.

«Семіотика – наука про знак, текст і механізми генерування значень – тривалий час розвивалася в універсалістському культурному ключі – у ролі основоположної філософії інтерпретативної діяльності» [1, с. 4].

Так, семіотика (від грец. *Σημειωτικός* (слово, що має дві складових ознаки від грец. *σημεῖον* – ознака, та грец. *σῆμα* – знак)) – наука, яка досліджує способи обміну інформацією, властивості знакових систем у людському суспільстві, природі або в самій людині. Іншими словами, семіотика – це теорія знаків та знакових систем.

«Знак є схематичним зображенням духовної сутності, тобто її проекцією або коагуляцією в матерії. Парацельс, описуючи магічні літери (*magia caracterialis*) у своєму творі «*Astronomia Magna*» (1571), стверджував, що накреслені знаки або букви володіють тією ж самою владою, що й мова. Імена або слова, що формуються за допомогою таких криптографічних дій, самі по собі є векторами, невіддільними від суті істот або ангелів, до яких вони належать, і володіють магічними силами і властивостями останніх. Якщо ми візьмемо до уваги концепції *magia naturalis* (природної магії), то такі криптографічні письмена можна вважати, методом застосування, крім інших теорій сигнатур і універсальних відповідностей» [2].

Семіотичне значення поняття «символ» реалізує нове слово як шифр, що є невід'ємною складовою криптографії. Давньогрецький полководець Еней Тактика у роботі «Про оборону укріплених місць» описує так званий «книжковий шифр» і спосіб перестановки букв у тексті за спеціальною таблицею, складеною ще в IV ст. до н.е. Відома також система шифрування за назвою «квадрат Полібія», у якій кожна буква заміняється парою чисел – її координатами у квадраті 5х5, куди попередньо у заздалегідь заданому порядку вписані букви алфавіту.

Вже тоді шифрована переписка використовувалася не тільки полководцями, але й церквою та вченими. Жерці шифрували тексти віщунів, а вчені – свої відкриття. Наприклад, Е. Шюре у книзі «Великі присвячені» зустрічається фраза про те, що завдяки великій праці, великою ціною добув Платон один з манускриптів Піфагора, що колись записував своє навчання не інакше, як таємними знаками і за допомогою різних символів [4, с. 45–57].

У Європі криптографія перебувала в стані застою аж до настання епохи Відродження. Застосовувалися шифрові системи, які були гранично простими. Фрази писалися по вертикалі або у зворотному порядку, голосні замінювалися точками, використовувалися іноземні алфавіти (наприклад, давньоєврейський і вірменський), кожна буква відкритого тексту замінялася наступною за нею буквою. Крім того, протягом усіх цих років криптологія була вражена хворобою, яка збереглася до більш пізнього часу, а саме переконаністю багатьох людей в тому, що криптографія і криптоаналіз є різновидами чорної магії.

З перших днів свого існування криптографія мала на меті заховати зміст важливих розділів письмових документів, що мали відношення до таких сфер магії, як ворожіння і заклинання. В одному з рукописів про магію, що датується III століттям, використовується шифр, щоб приховати важливі частини чаклунських рецептів. Криптографія часто була на службі магії в часи середньовіччя, і навіть в епоху Відродження за допомогою шифрів алхіміки засекречували важливі частини формул отримання філософського каменя.

Твори з криптографії потрапили в розділ магічних творів, тому, що вони були включені в єдину систему окультної філософії, яка розвивалася в період з XV по XVII століття: згідно з цими уявленнями, всесвіт складений з багатовимірних дзеркал, у яких нескінченно різні існуючі речі відображають один одного, при цьому, будучи пов'язані, величезною кількістю взаємозв'язків. Виходячи з даних уявлень, знак, написаний магом, згідно з власними ж властивостями пов'язаний із закликанням небесних істот або з небесним тілом, яке є ніби посудом, в якому ця істота міститься. Таким чином, знак є своєрідним проявом або безпосереднім вираженням ангела.

У системі Мартінеса де Паскуаллі (XVIII століття) теург у своїй «кімнаті для Церемоній» креслив на лляному килимі знак, або, як його називають мартінезісти, «ієрогліф», який повинен був «відповідати» ангелу, і який вибирався серед 2400 ієрогліфів зі Списку, (цей Список все ще зберігається в архіві «Прунелла де Льєрена» в Муніципальній Бібліотеці Ліона). Якщо Операція відбувалася належним чином, в такому випадку, через короткий проміжок часу, в кімнаті перед Теургієм повинен був з'явитися той чи інший ієрогліф, який світиться. Якщо ж з'являвся якийсь інший ієрогліф, то це означало, що пізніше теург повинен буде переглянути Список для того, щоб знайти в ньому ієрогліф, який перед ним з'явився. Очевидно, що ці гліфи (ієрогліфи) розуміли, (як у системі Паскуаллі, так і в інших подібних їм системах), як знаки, які потрібно було зображати і використовувати теургію під час ритуалу, а також як знаки, посилаються ангелами, яких викликали під час ритуалу призивалися.

Подібність між магією і криптографією підкреслювалося іншими факторами. Крім криптографії, таємничі символи використовувалися в таких зрозумілих лише присвяченим областям магічних знань, як астрологія і алхімія, де, подібно знакам відкритого тексту, кожна планета і кожна хімічна речовина мали спеціальний знак. Як і зашифровані слова, заклинання і магічні формули, на кшталт «абракадабри», походили на нісенітницю, але насправді були кодовані прихованим значенням.

Багато людей, які хвалилися своєю здатністю розгадувати шифри, одночасно вихвалялися і умінням чути людські голоси, будучи глибоко під землею, або даром телепатії. Природно, що згодом ці дві галузі стали обговорюватися разом, оскільки вони завжди розвивалися у тісному взаємозв'язку.

Думка про те, що криптографія є за своєю природою чорною магією, обумовлена і поверхневою подібністю між крипто аналізом та ворожінням. Шифрування тексту видавалося такою справою, що й одержання знань шляхом вивчення розташування зірок і планет, довжини ліній і місць їх перетину на долоні, нутрощів овець, положення кавового осаду в чашці. Видимість брала гору над реальністю. Простодушні вбачали магію навіть у звичайному процесі розшифрування. Інші, більш досвідчені, бачили її в криптографії, оскільки розтин чогось глибоко захованого здавалося їм незбагненним і надприродним. Знавцям поезії добре відомий такий досить широко використовуваний у той час прийом тайнопису, як акровірш, у якому приховуване повідомлення утворюють початкові букви віршованих рядків.

У XVI ст. у тлумаченні терміну «криптографія» відбувався еволюційний прорив, оскільки цей термін вперше було ототожнено з терміном «стеганографія». Даний термін ввів абат Йоганн Тритемій у Німеччині. Він розвинув ідею Альберта Великого щодо значення езотеричності коду, та використав пікторальну спіраль або багатоалфавітну заміну.

У Російській імперії (хоча тайнопис використовувався вже з XII–XIII столітті) офіційною датою появи криптографії вважається 1549 рік (за царювання Івана IV), коли було утворено «посольський наказ», при якому було «цифрове відділення». Шифри використовувалися такі ж, як на заході – значкові, заміни, перестановки. Петро I пізніше повністю реорганізував криптографічну службу, створивши Посольську канцелярію. У цей час з'являються спеціальні коди для шифрування «цифрові абетки».

На початку XVI століття Маттео Арджентi, криптограф папської канцелярії, винайшов код, відповідно до якого можуть замінятися не тільки букви, але й склади, слова, навіть цілі фрази. Десь у цей же час з'являється й числовий код. Це зумовлює та розширює поняття езотеричності коду: криптографія характеризується як тайнопис, а кодування як елемент знаково–символьного аналізу даного тайнопису.

Наступним етапом розвитку криптографії можна вважати 1563 рік, коли у своїй книзі «Про таємну переписку» італійський натураліст Джованні Порта описав біграмний шифр, у якому здійснюється заміна не однієї букви, а пари букв. У своїй книзі Порта наводить приклади списків імовірних слів з різних областей знання, істотно передбачивши те, що згодом криптологи виведуть «методом імовірного слова». Приблизно в той же час французький посол у Римі Блез Віженер, ознайомившись із працями з криптографії, пише книгу «Трактат про шифри» (1585 р.), у якій він пропонує застосовувати відкритий або шифрований текст і висловлює думку про те, що «всі речі у світі являють собою шифр. Вся природа є просто шифром

і секретним листом». Пізніше цю думку повторять і Блез Паскаль, і батько кібернетики Норберт Вінер [4].

Висновки дослідження. Стійкість шифру сьогодні оцінюється обсягами обчислень, які необхідні для його розкриття. Вважається, що ключ шифрування досить стійкий, якщо всі відомі способи його відшукати настільки складні, що вимагають більше часу, ніж простий перегляд усіх можливих ключів.

Всі ми сьогодні, іноді навіть не підозрюючи про це, застосовуємо засоби захисту інформації. Ми шифруємо повідомлення електронної пошти, користуємося інтелектуальними банківськими картками, ведемо розмови по закритих каналах зв'язку й тощо. Щоразу виникає питання чи надійний захист? Але й це елементарне питання не так просто правильно сформулювати. Як виміряти стійкість захисту? Чого ми прагнемо досягти – сховати факт переписки? Зашифрувати зміст? Засекретити імена адресатів? Не дозволити супротивнику спотворити інформацію? На всі ці запитання та багато інших відповідь має історія розвитку криптографії, коду, символу, знаку, шифру.

Список використаних джерел

1. Павлюк Л. С. Знак, символ, міф у масовій комунікації. – Львів: ПАІС, 2006. – 120 с.

2. Жиль де Поп. Криптография в Западном эзотеризме [Электронный ресурс] / Жиль де Поп. – Режим доступа: http://www.teurgia.org/index.php?option=com_content&view= article&id=995:l–r–&catid=18:2009–12–21–14–45–31&Itemid=7

3. F. Edvard Hulme. Cryptography, Principles and Practice of Cipher Writning. – London, 2013. – 198 p.

4. Kahn D. The Codebreakers. – New York, 1973. – 473 p.

References

1. Pavljuk L. S. Znak, symvol, mif u masovij komunikacii'. – L'viv: PAIS, 2006. – 120 s.

2. Zhil' de Pop. Kriptografija v Zapadnom jezoterizme [Jelektronnyj resurs] / Zhil' de Pop. – Rezhim dostupa: http://www.teurgia.org/index.php?option=com_content&view= article&id=995:l–r–&catid=18:2009–12–21–14–45–31&Itemid=7

3. F. Edvard Hulme. Cryptography, Principles and Practice of Cipher Writning. – London, 2013. – 198 p.

4. Kahn D. The Codebreakers. – New York, 1973. – 473 p.

Mykhalchuk A. O., *graduate student of Cultural Studies, Eastern National University Lesya Ukrainka (Ukraine, Lutsk), Potter15@list.ru*

Problem cryptography: semiotic dimension

This article explores the features cryptographic code, the concept «cypher» and his semiotic interpretation. Characterized value of philosophical terms «character» and «semiotic». Substantiated that the code is an integral part of cryptology, lying in the context semiotic approach and reduced to logical thinking whole variety of cultural values. Signs and symbols represents a combination of different areas of media and cultural space metaphysical generalization of mathematics, physics, astronomy and architecture. But there is a more specific meaning cryptography: its methods used for establishing the connection between the earthly world and the world is in heaven.

Keywords: *sign, symbol, code, cryptography, semiotics, cipher, magic.*

Михальчук А. О., *аспирант кафедры культурологии, Восточноевропейский национальный университет им. Леси Украинки (Украина, Луцк), Potter15@list.ru*

Проблема криптографии: семиотический аспект

Исследуются особенности криптографического кода, суждение понятия «код», и его значение. Экспликуются философские термины «символ» и «знак». Обосновывается, что код является неотъемлемым элементом криптологии, который лежит в контексте семиотического подхода, и сводится к логической цепочки всего разнообразия культурных ценностей. Знак и символ олицетворяет собой сочетание различных сфер медиа культурного пространства и метафизических обобщений математики, физики, астрономии и архитектуры. Однако существует и более специфический смысл криптографии: ее методы использовались для установления связи между земным миром и Миром Небесным.

Ключевые слова: *знак, символ, код, криптография, семиотика, шифр, магия.*

* * *

УДК 130.2

Попович М. Д.,
доктор філософських наук, доцент, завідувач кафедри історії і філософії, Подільський державний аграрно–технічний університет (Україна, Кам'янець–Подільський), mykhai@ukr.net

КОМУНІКАТИВНИЙ РЕСУРС ЛЮДСЬКОЇ СВОБОДИ ЗА УМОВ ГЛОБАЛІЗАЦІЙНИХ ВИКЛИКІВ

Мова йде не просто про позбавлення іншої людини від непосильних (а до того ж, як правило, зайвих) комунікацій. Комунікація, в якості повідомлення, завжди може надати повідомленню інший сенс, але це відразу ж видно в соціальних взаєминах. Те, що в таких випадках не спрацьовує, – це принцип комунікації, а саме відмінність інформації та повідомлення, що додає самому повідомленню характер події, що вимагає реакції. Вже на рівні інтимних соціальних взаємин проявляє себе принципова залежність реалізації соціальної свободи у зовнішній соціальній інстанції – нехай це буде навіть кохана людина. Сама будучи багатофункціональною, мораль може лімітувати можливості функціональної специфікації. У такому випадку соціальне взаємопроникнення не може бути виокремлене без урахування міжлюдських відносин. З іншого боку, мораль накладає свої обмеження і на сферу інтимних взаємин. Адже точно так само неможливо поглиблювати інтимність між людьми, якщо вона пов'язана з суспільною мораллю. З точки зору теорії соціальних систем культура є швидше широким полем можливостей, які розкриваються у комунікації людини. Це і є нашою головною вихідною методологічною позицією, яку у подальшому ми рекомендуємо до застосування у соціальних та гуманітарних дослідженнях не стільки у режимі жорсткого методу, який форматує дослідження, скільки у якості наскрізної ціннісно–світоглядної настанови. На зміну моделі уніфіковано–стандартизованого світу (єдиного і одноманітного) приходять нові концепції глобалізації, що містять у собі ідею збереження культурного розмаїття в житті людей.

Ключові слова: *соціальна комунікація, свобода, глобалізація, теорія соціальних систем, теорії глобалізації.*

На основі синтезу багатьох спеціальних знань та дисциплін, поєднуючи історичні, соціологічні, економічні, історико–філософські матеріали, Ю. Габермас здійснив спробу історичної реконструкції моделей соціальних відносин у час зародження простору відкритого публічного спілкування. Він показав, за яких умов, коли та як раціонально–критичні дебати громадян щодо суспільних проблем, а також аргументи, що народжувались у цих дебатах, почали складати авторитетну основу для прийняття політичних рішень; яким чином громадськість (публіка) і притаманна їй «громадська думка» перетворилися на чинник політики та соціально–економічного життя в європейській культурі [3, с. 14].

Насамперед, комунікативними передумовами людської свободи можна назвати наступні: 1) публіка – соціальний замовник і добровільний споживач відкритих комунікаційних продуктів та послуг в особі громадянського суспільства; 2) автономні соціально–комунікаційні інститути, вільні від державного втручання та ідеологізації; 3) ліберально–демократичне державне регулювання, яке охороняє права і свободи індивідів, груп та спільноти в цілому; 4) суб'єкти господарської діяльності, які фінансово підтримують засоби масової комунікації відкритого типу.

Всі ці передумови пов'язані з конкретними соціальними інститутами культури, зразком яких постають передусім ліберальна преса та демократичне урядування. Передусім, успішне функціонування таких інститутів має спиратися на поширення у суспільстві відповідного типу ліберально–демократичного світогляду. Своєю чергою останній разом з першими втілюють ту демократичну нормативність, яку у своїх текстах обґрунтовували ще І. Кант [4] та засновники американської демократії, про що писав Макс Вебер [2]. А вони є лише одними з можливих організаційних та інституційних втілень демократії