

**Андрій Михальчук**

*Східноєвропейський національний університет ім. Лесі Українки, Україна*

## **КРИПТОГРАФІЧНІ КОДИ У КОНТЕКСТІ СУЧАСНОЇ МЕДІА-КУЛЬТУРНОЇ ДІЯЛЬНОСТІ**

**Andrii Mykhalchuk**

*Lesya Ukrainka Eastern European National University, Lutsk, Ukraine*

## **CRYPTOGRAPHIC CODES IN THE CONTEXT OF MODERN MEDIA-CULTURAL ACTIVITY**

The article deals with philosophical, semiotic and social aspects of the value of cryptographic codes in the media-cultural space of our time. A structured analysis of the code as an element of the information space is carried out and the code is compared with the evolution of the computer and computer technologies in 20th-21st centuries. It is substantiated that modern security algorithms are part of the semiotic concept of code in its modern interpretation (modern systems and software products). The information space is rapidly evolving: the progress of the computer and network, telecommunications, and the diagnosis of information security are all factors of the modern media information society. The system of signs, which are in the form of a computer code, makes it possible to study the «mystery» of the nature of the cipher and its significance in nowadays media-cultural activities.

**Keywords:** cryptography, media culture, code, mining system, philosophy of algorithms, virtual reality.

**Постановка наукової проблеми та її значення.** Сучасний інформаційний простір є надзвичайно важливим інструментом у постіндустріальному суспільстві. У ХХІ ст. комп'ютеризований світ існує як одна мережева система, де код відіграє надзвичайно важливу роль в будь-якій сфері діяльності людини. Будь-яка сучасна система кібербезпеки складається із різноманітних символів, що утворюють багатофункціональний інструмент, який сьогодні відомий як програма або програмний продукт.

Більшість структурованих елементів комп'ютерного коду є запозиченими елементами із різних областей науки, культури, релігії, що в свою чергу сприяє розширенню процесів пізнання людиною нашого світу й космосу за допомогою криптографії та комп'ютера.

**Аналіз досліджень із цієї проблеми.** В постіндустріальну епоху людство перейшло від традиційних культурних парадигм еволюції до прискореного розвитку інтелекту по експоненціальній кривій, де головним чинником стає інформаційний простір мас-медіа. Саме завдяки постійним вдосконаленням комп'ютера та поширенням всесвітньої мережі Інтернет гостро постає проблема безпеки даних. Більшість відомих світових компаній, таких як Apple, Intel, IBM, Samsung, Sony, Xiaomi інвестують багатомільйонні прибутки у розвиток безпечових систем захисту інформації. Даніел Белл зазначає, що «знання та інформація є стратегічними ресурсами трансформації постіндустріального суспільства, де важливим елементом є обробка інформації та розставлення найбільш важливих пріоритетів для розкриття власного потенціалу»<sup>1</sup>. Сьогодні інформаційна безпека є надзвичайно важливим фактором у підтриманні балансу на Землі та пошуку нових механізмів у дослідженні «невідомих» людству знань.

Серед дослідників, які займались проблемами інформаційних кодів належать Д. Белл, У. Еко, М. Кастельс, Н. Кирилова, Н. Луман та криптографічних кодів М. Адаменко, С. Зінгх, Д. Канн, П. Хеменвей, Б. Шнайер.

**Мета статті.** Метою дослідження є аналіз криптографічних кодів та їх значення у медіа-культурній діяльності сучасності.

<sup>1</sup> Белл, Д. (1986). Социальные рамки информационного общества. *Новая технократическая волна на Западе*. Москва: Прогресс, 330-342.

Завдання: проаналізувати філософсько-семіотичний та соціальний аспекти значення криптографічних кодів у медіа-культурній діяльності.

**Викладення основного матеріалу й обґрунтування отриманих результатів дослідження.**

Загальною характеристикою інформаційного простору суспільства є те, що створюється нова інформаційна сфера, базовими елементами якої є надсучасний процесор та інтелект. Значним кроком у сфері комунікації беззаперечно слід вважати створення комп'ютера, як поєднання філософської ідеї, електронної пам'яті та обчислювальних програм.

Комп'ютери різного ступеня складності та потужності активно використовують уряди, секретні служби, армії, державні та комерційні установи, а також суспільство для виконання найрізноманітніших задач. У результаті розвитку комп'ютерних технологій велика кількість інформації мусить залишатись конфіденційною, зокрема такі данні, як коди доступу балістичних ракет, ядерних установок у армії, інформація про акції на великих фондових біржах, інформація щодо банківських рахунків тощо. Тому необхідність у різноманітних системах захисту щодня тільки збільшується.

Ера «комп'ютеризації» розпочалась під час Другої світової війни, коли у фашистській Німеччині вперше був розроблений прототип комп'ютера в моделі Z3, яку створив німецький комп'ютерний інженер Конрад Цузе. Однак офіційно першим вважається запуск електронно-цифрової обчислювальної американської машини ENIAC у США у 1946 р.

Процеси аналізу обробки обчислювальних даних були повністю побудовані на математичних обрахунках, логіці та філософських ідеях, що поступово втілювались у фізико-інженерний шедевр – комп'ютер. Із розвитком кожного покоління комп'ютерна індустрія потребувала ще більшого дослідження знакових процесів, за допомогою яких людина здатна була б комунікувати з машиною доступною їй мовою двійкової системи Г. Лейбніца<sup>1</sup>. Семіотично-інформаційна модель втілювала в життя нові інформаційні виклики, що здатні були б опрацьовувати дані та миттєво їх передавати. Згідно з теорією комбінаторики Г. Лейбніца, криптографічні коди є графами, що здатні трансформуватись в більш глибокі кодові структури, зображуючи код як багатоієрархову систему знаків та знакових змінних.

Умберто Еко зазначав: «Доволі очевидним є те, що ми отримали тільки ядро певного, більш розширеного розгалуження, завдяки якому ми в будь-який час, коли в цьому виникає “оперативна необхідність”, зможемо по новому трактувати більш глибокі структури»<sup>2</sup>. Умберто Еко детально описує структуру  $S_n$  та перехід від коду до метакоду, як нового етапу еволюції людства на шляху до семіотичного «структуралізму». З точки зору семіотики наповнення новим змістом окремих знаків та знакових систем дозволить досліджувати об'єкти у трьох аспектах: семантики, синтактики та прагматики. Перші кроки до розуміння цих процесів були зроблені під час створення комп'ютера першого покоління.

Аналізуючи ці структури, доцільно навести паралель із архітектурою комп'ютера. Маловідомо, що процеси які визначені філософсько-теоретичною семіотикою, активно використовуються в практиці комп'ютерного моделювання. Структура пам'яті сучасного комп'ютера побудована на структурі «push» та «pop», що в програмуванні більш відоме як «стек», який побудований на принципах LIFO. На нашу думку, аналогами цієї процедури кодування є процеси, описані в семіотичній теорії У.Еко як «emis» та «eris». Семіотика структуралізму, яка описана у праці Умберто Еко «Відсутня структура» зображає код як знакову модель, що виконує певну функцію щодо інформації. Ця теорія дещо відтворена в сучасній фон Нейманській архітектурі комп'ютера, що експлікує код із двійковою системою Г. Лейбніца. Комп'ютерний код набуває певної форми (алгоритми), який виконує задану функцію створює ядро (інформацію) та дозволяє перенести це ядро від одного користувача до іншого. Слід припустити, що криптографічний код є системою мнемонічних знаків, які шукають певні зв'язки між знаками та об'єктом (тілом та його функціями) та інтерпретатором (джерелом, який здатний виконувати функцію кодування та декодування). Більшість структурних процесів кодування базуються на основних значеннях семіотики, в яких знаки можуть виконувати головну атрибутику (індекс) та допоміжну (символ).

<sup>1</sup> Лейбниц, Г.В. (2005). *Письма и эссе о китайской философии и двоичной системе исчисления*. Москва, 404.

<sup>2</sup> Еко, У. (2006). *Отсутствующая структура. Введение в семиологию*. СПб.: Симпозиум, 15.

Кінець ХХ століття відзначився небувалим кроком у майбутнє розвитку всесвітніх інформаційно-комунікаційних систем – Інтернет став третім еволюційним каналом зв'язку, що докорінно вплинув на розвиток сучасних систем мас-медіа.

Більшість семіотичних та базових ідей поняття «Інтернет», описані в загальному емпірично-математичному аналізі у книзі Р.Снеддена «Винаходи ХХ ст. Інтернет». Досліджуючи проблему Інтернету та його концепцій, варто наголосити більш детально на філософських ідеях та безпосередньо результатів заснування тої всесвітньої мережі, яка відома нам сьогодні.

Інтернет-комунікації – це лише один із засобів та способів передачі даних, що виконують ті криптографічні алгоритми, які дозволяють протоколи відповідного захисту даних. Ось як відомий американський криптограф Брюс Шнайер описує значення криптографічних алгоритмів: «Криптографічний алгоритм, також має назву “шифр”, представляє собою математичну функцію, яка використовується для шифрування та дешифрування. Якщо безпечність алгоритму створена на збереженні самого алгоритму в секреті – це обмежений алгоритм.... Велика або змінна група користувачів не може використовувати такі ж алгоритми, та якщо коли-небудь користувач залишає певну групу, її члени повинні переходити на інший алгоритм»<sup>1</sup>.

Більшість алгоритмів записані в такому вигляді, щоб проста людина не зрозуміла записаного навіть володіючи необхідним кодом до цього алгоритму. Ітераційна послідовність створює настільки своєрідний мнемонічний код, що під дією додаткових чинників (наприклад майнфреймів), даний код може еволюціонувати в метакод, тобто «код в коді». З точки зору семіотики, такий метакод є комунікаційним інформаційним чинником, який дозволяє суспільству, під дією кодів шифрувати дані на зовсім іншому рівні (кодування психіки людини), за допомогою багатьох інструментів інтернет-комунікацій. До таких інструментів можна віднести відео-конференції, відправлення повідомлень електронною поштою, перегляд аудіо та відео-файлів у спеціально створених доменних точках (наприклад Youtube), спілкування в соціальних мережах і т.п. Більшість технологій, зокрема такі як мобільний телефон, за допомогою Інтернет-комунікацій повністю переходять у так званий віртуальний світ, де більшість життєвих процесів замінює двійкова система.

Ось як відомий німецький соціолог Ніклас Луман зіставляє семіотику медіакультури з комп'ютером: «... комп'ютер змінює співвідношення (доступної) поверхні та глибини. Тепер справа більше не торкається основ лінеатури, яка побудована на висловлюванні передбачень або про орнаменти, що підкреслюють дане значення. Поверхність тепер – це екран монітору, що, припускаючи граничне обмеження, звертається до людських почуттів; глибина в свою чергу, навпаки, невидима машина, яка сьогодні здатна в один момент перебудувати себе саму, наприклад, реагуючи на запити користувача. Зв'язок поверхні та глибини може активізовуватись в цьому випадку під дією команд, що вказують машині, що слід виводити на екрані або сформулювати в своєрідному вираженні. Однак зв'язок продовжує бути невидимим.... Лише тому можна окреслити машину в якості “Віртуальної реальності”»<sup>2</sup>.

Відомий український дослідник М. А. Журба аналізує віртуальну реальність, як вид буття, що вживається у двох значеннях: як позначення усіх форм матерії (речовинного світу); як ідеальний продукт матеріального світу. «Перша реальність – реальність об'єктивна, якій протиставляється реальність суб'єктивна. Друга реальність, що включає у себе світ духовно-ідеальний, з якою ми маємо справу, коли відходимо від речовинного світу, дає можливість зводити у ранг можливого ілюзії, фантазії тощо»<sup>3</sup>.

Відомий іспанський медіа-теоретик Мануель Кастельс має дещо іншу думку щодо «віртуальної реальності». Як стверджує іспанський соціолог, людство живе в умовах специфічної, виокремленої культури, яка є віртуальною, оскільки будується на віртуальних процесах медіакомунікації, що є повністю автоматизованою. Культура є реальною, а не уявною, що створює фундаментальну дійсність, опираючись на те, як кожна людина планує власне життя; як вона контактує із соціумом, що вона прагне пізнати та яку роль вона виконує у даному суспільстві. З точки зору М. Кастельса, віртуальність – це і є людська реальність. Саме віртуальна реальність є

<sup>1</sup> Шнайер, Б. (2002). *Прикладная криптография*. Москва: Триумф, 18.

<sup>2</sup> Луман, Н. (2005). *Медиа коммуникации*. Москва: Логос, 137–138.

<sup>3</sup> Журба, М.А. (2014). Віртуальна реальність: різновекторні пошуки. *Гілея: науковий вісник*, 86, 172.

відмінною рисою культури інформаційно-цифрової епохи, оскільки саме кодом, ми в більшості випадків приносимо нашому існуванню сенс<sup>1</sup>.

Багато семіологів та криптографів не тільки визначили поняття феномену «Інтернет», а й продовжують теоретично обґрунтувати інформаційний простір медіакультури ХХІ ст. Власне сам процес віртуалізації слід вивчати не як безпосередній результат комп'ютеризації світу, а з позиції еволюційного шляху людини, де коди тісно переплітаються з повсякденним життям.

Будь-які інтернет-комунікації є настільки полігамними, що людина сама здатна здійснювати процес кодування та декодування інформації з будь-яких пристроїв носіїв інформації (комп'ютер, телефон, планшет тощо). Аналізуючи інтернет-комунікації та його значення у формуванні сучасної медіакультури, слід відокремити ті інструменти, які здатні впливати на людські процеси мислення. Система телекомунікацій включає в собі низку способів передачі інформації. Сьогодні система функціонує на основі багатьох чинників та може надавати наступні послуги: електронна пошта, перегляд новин, поштова розсилка / смс розсилка, віддалений доступ до комп'ютера, різноманітні сеанси зв'язку (Billing system), безпосередній пошук інформації в оперативно-аналітичному режимі; спілкування з друзями / рідними (Google Chat, Internet Relay Chart, Internet Calling), мійнінг система або система інтернет-валют (електронна криптовалюта Bitcoin) та інші системи і процеси, що побудовані на кодуванні та різноманітних криптографічних алгоритмах.

Сьогодні кодом системи мас-медіа є відмінність між інформацією та неінформацією, віртуальністю та реальністю. Як зазначає Ніклас Луман: «Інформація – це позитивне значення, предметне означення, за допомогою якого система маркує можливість свого власного функціонування. Однак, щоб мати можливість розглядати будь-що в якості інформативного або неінформативного, повинна існувати можливість приймати будь-що за неінформативне.....»<sup>2</sup>.

Концепцією Н.Лумана є аналіз факторів, що впливають на мас-медіа та створюють спеціальне інформаційне поле, що під дією комунікаційних та лінгвістичних особливостей розширює світоглядне розуміння процесів у медіакультурі.

Наприклад, ми хочемо відправити два повідомлення з різним об'ємом даних. Перше повідомлення займає, наприклад, 2 біти (вибір із 4 рівно вірогідних можливостей) та друге повідомлення, що займає 3 біти (вибір із 8 рівно вірогідних можливостей). Відмінністю даних повідомлень з точки зору кодування є лише прорахування більшої кількості варіантів. У другому повідомленні інформації є більше, а отже, вихідна ситуація є менш визначеною. У даному випадку інформація – є свободою вибору автора під час написання повідомлення, де ключову роль відіграють лінгвістичні особливості, специфіка, розв'язка події, атрибутика, що є важливим для відправника. Людський мозок здатний опрацювати одночасно не два, вісім, шістьдесят чотири, п'ятсот дванадцять варіантів, а мільйони комбінацій, що здатні моделювати ту чи іншу ситуацію, притаманну лише кодам. Комп'ютерний код є системою змінних даних, які під зміною одного або декількох функцій виводять необхідний результат, але в тисячі разів повільніше, ніж людський мозок.

Для досягнення власних цілей хакери щодня створюють різноманітні зловмисні програми, так звані віруси, хробаки, троянські коні тощо. З точки зору семіотики – це «спосіб кодування нашого сприйняття світла та безпосереднє відтворення його на полотні»<sup>3</sup>.

Звичайні шкідливі програми (віруси) здатні, наприклад, скопіювати (клонувати), знищити або видозмінити будь-який файл. У даному випадку код виконує одночасно функцію програми та файлу. Зв'язок, що поєднує обидва об'єкти, є тонкою поверхнею (алгоритмом) відтворення світла та тіней. Більшість вірусів кожна людина може підхопити безпосередньо з Інтернету. На основі описаних факторів є очевидним те, що у справі захисту даних, які зберігаються в певному місці, криптографія або теорія інформації отримала нове, практично не досліджуване поле діяльності, що побудоване на спеціальних алгоритмах захисту – семантики знаку.

Сьогодні розшифрування повідомлення без знання комп'ютерного алгоритму шифрування та наявності ключа відповідної довжини є завданням практично неможливим. Залежно від принципів побудови алгоритмів шифрування коду ділиться на 2 групи: симетричне або асиметричне.

<sup>1</sup> Кастельс, М. (2004). *Галактика Інтернет: Размышления об Интернете, бизнесе и обществе*. Екатеринбург: У-Фактория, 237–239.

<sup>2</sup> Луман, Н. (2005). *Реальность масс-медиа*. Москва: Праксис.

<sup>3</sup> Эко, У. (2006). *Отсутствующая структура. Введение в семиологию*. СПб.: Симпозиум, 164.

Під час використання симетричних алгоритмів використовується однаковий ключ. Цей алгоритм отримав широке розповсюдження через власну простоту. Вважається, що даний шифр був не чим іншим як філософською ідеєю Готфрида Лейбніца, який вважав це «природою речей». Однак, сьогодні ця ідея відома криптоаналітикам як алгоритми DES, 3DES, IDEA та Blowfish. Генерацією такого типу алгоритмів є ланцюги кодів, що утворюються в метакод (пейзаж імпресіоністів або експресіоністів), що підміняє стиль роботи та задумку автора в період безпосередньої відправки повідомлення.

Ще одним типом шифрування даних є асиметричний алгоритм, тобто алгоритм з різними ключами. Задумкою даного шифру є ренесансна ідея Леонардо да Вінчі «гри світла та тіней». Побудова такого алгоритму полягала у рівномірному розділенні ключа на дві частини, що утворювали одне ціле, як в алхімії «дзеркальна видозміна». Будь-який код чи безпосереднє кодування було б неможливим без знання семіотики знаку, алхімії, криптографії та науки, що уособлюють дерево та філософії, що уособлює коріння цього дерева.

Сьогодні криптографія досягає своєї вершини популярності та здатна впливати на всі процеси в будь-якій сфері науки та суспільства. Із набуття масового поширення технологій всесвітньої мережі, постала перед філософією, криптографією та безпосередньо науки нове питання – «електронна валюта».

Економіка фактично заснувала таке поняття як валюта, однак із розвитком телекомунікаційних систем поступово набирає популярності ознака криптовалюти. Прослідкувавши еволюції валюти від монет та банкнот до банківських платіжних систем попит на «електронну валюту» починає набирати популярності в суспільстві, безпосередньо пов'язаних із мережею Інтернет.

У XXI ст. ми спостерігаємо за повноцінно новою платіжною системою, яка має низку відмінностей серед інших електронних валют. Код, на основі якого фактично створена нова платіжна «майнінг» система, стала новим заробітком у сфері індустріалізації медіакомунікації.

Перші згадки про криптовалюту як альтернативної платіжної системи розрахунків починаються з 1998 р., філософську ідею, створення якої належить японському криптографу та програмісту Вей Даю. Він вперше запропонував нову модель ринкового механізму «b-money». До проекту також долучились Нік Сабо та Хел Фінні. У 2008 р. закладено початок створення криптовалюти людиною або групою людей під псевдонімом Сатосі Накамото – файл із розробленим кодом та алгоритмом безпекових протоколів та загальні принципи роботи нової платіжної системи у вигляді однорангової мережі. Код почав еволюцію у сфері цифрової валюти та одночасно розширив інформаційне поле досліджень медіакультури сучасності.

Принципом роботи криптовалюти «Bitcoin» є найбільш розгалужена комп'ютерна мережа, що виконує роботу обчислювальних машин та проводить великі обчислювальні обрахунки, на які не здатний один «суперкомп'ютер». Філософська ідея полягає в тому, що «майнінг» система створена для того, щоб шукати вирішення надзвичайно важливих питань людства. Система виконує дві головних функції – пошукову та обчислювальну, де кодування є ядром цієї системи.

Пошукова функція здійснює збір великих масивів метаданих із усіх комп'ютерних мереж та виконує функцію розбивання великого завдання на тисячі менших операцій, які здатний виконати один комп'ютер із необхідними для цього ресурсами. Усі отримані дані збираються в одне місце – спеціальний сервер, який виконує обробку отриманих даних. Із точки зору семіотики – це зображає пошук інформації в природі, де під дією натхнення побаченого, художник пише картини чи скульптор створює скульптуру.

Обчислювальна або аналітична функція здійснює всі необхідні дії за допомогою багаторівневих кодових алгоритмів для отримання першочергового результату. Майнінг системою було досліджено декілька важливих проектів, зокрема таких як обробка даних виверження вулканів, сейсмічна активність, дослідження ДНК людини, розробка диску-генів людини, з інформацією якої людина здатна вилікуватись від смертельних хвороб, що прогресують на ранніх стадіях, тощо.

У статті Вахрушева Д.С. та Железова О.В. криптовалюта як феномен сучасної інформаційної економіки має декілька спільних факторів із інформаційною безпекою: по-перше, наявність децентралізованої мережевої емісії криптовалют; по-друге, створення зашифрованою програмного коду, який зберігає всі необхідні дані виключно на серверах; по-третє, осучаснена ідентифікація

користувачів для управління грошовими коштами та потоками<sup>1</sup>. Якщо розглядати криптовалюту як масове явище, то варто проводити аналогії з наявними електронними платіжними банківськими системами. На нашу думку, криптовалюта – це еволюція платіжних систем (наприклад в порівнянні з Webmoney) є наступним поколінням електронних платіжних систем, які в свою чергу можуть обслуговуватись не тільки банківськими установами, а й простими користувачами, власне як фінансового елементу медіа-комунікації.

У статті Бречко О.В. визначає підходи обґрунтування феномену криптовалюти, зважаючи на технічні характеристики безпекових протоколів біткоїнів: як розподілена система записів (операцій); як інноваційна мережа платежів; як технологія, за допомогою якої здійснюються товарно-обмінні операції<sup>2</sup>. Опираючись на дослідження науковців можемо стверджувати, що криптовалюта є похідною сучасного криптографічного коду як фінансового чинника віртуальної реальності.

Майнінг система – це процес використання обчислювальних потужностей комп'ютерних систем для створення ланцюга транзакцій безпосередньо криптовалюти. У кожному ланцюгу, що складається із блоків, перша транзакція в списку є особливою транзакцією. Якщо майнери зупинять власну роботу або Інтернет перестане працювати, криптовалюта зникне.

**Висновки досліджень.** Криптографічний код сьогодні став багатогранним об'єктом досліджень. Різноманітні комп'ютерні коди є новою проблемою в еру комп'ютерних технологій. Інформаційний простір швидко еволюціонує: прогрес комп'ютера та мережевих вузлів, телекомунікації, діагностики інформаційної безпеки – усе це чинники сучасного інформаційного медіа суспільства. Система знаків, що набуває форми комп'ютерного коду уможлиблює дослідження «таємниці» природи знаку та його значення в медіа-культурній діяльності XXI ст.

#### References:

1. Bell, D. (1986). Social'nye ramki informacionnogo obshhestva [i Social framework of the information society]. *Novaja tehnokraticheskaja volna na Zapade* [A new technocratic wave in the West]. Moscow: Progress.
2. Brechko, O.V. (2017). Kriptovaljuta jak fenomen novoї finansovoї infrastrukturi: problematika teoretichnogo osmyslenja ta praktichnogo vikoristannja [Cryptovolume as a phenomenon of a new financial infrastructure: the problem of theoretical understanding and practical use]. *Ekonomichnij analiz* [Economic analysis], 27, 3, 144-150. [in Ukrainian].
3. Vahrushev, D.S., Zhelezov, O.V. (2014). Kriptovaljuta kak fenomen sovremennoj informacionnoj jekonomiki: problemy teoreticheskogo osmyslenija [Crypto currency as a phenomenon of modern information economy: problems of theoretical comprehension]. *Internet-zhurnal Naukovedenie* [Internet Journal of Science], 24, Vypusk 5, 1-9. [in Russian].
4. Zhurba, M.A. (2014). Virtual'na real'nist': rizinovektorni poshuki [Virtual reality: multi-vector searches]. *Gileja: naukovij visnik* [Gilea: Scientific Bulletin], 86, 171-175. [in Ukrainian].
5. Lejbnic, G.V. (2005). *Pis'ma i jesse o kitajskoj filosofii i dvoichnoj sisteme ischislenija* [Letters and essays on Chinese philosophy and binary number system]. Moscow. [in Russian].
6. Kastel's, M. (2004). *Galaktika Internet: Razmyshlenija ob Internete, biznese i obshhestve* [Galaxy Internet: Reflections on the Internet, Business and Society]. Ekaterinburg: U-Faktorija. [in Russian].
7. Kirilova, N.B. (2006). *Mediakul'tura: ot moderna k postmodernu* [Media culture: from modernity to postmodernity]. Moscow: Akademicheskij Proekt. [in Russian].
8. Luman, N. (2005). *Media kommunikacii* [Media Communication]. Moscow: Logos. [in Russian].
9. Luman, N. (2005). *Real'nost' mass media* [The reality of the media]. Moscow: Praxis. [in Russian].
10. Jeko, U. (2006). *Otsutstvujushhaja struktura. Vvedenie v semiologiju* [Missing structure. Introduction to Semiology]. SPb.: Simpozium. [in Russian].
11. Shnajer, B. (2002). *Prikladnaja kriptografija* [Applied Cryptography]. Moscow: Triumf. [in Russian].
12. Hulme, F. E. (2013) *Cryptography, Principles and Practice of Cipher Writing* [in Russian]. London. [in English].
13. Kahn, D. (1973). *The Codebreakers* [in Russian]. New-York. [in English].

<sup>1</sup> Вахрушев, Д.С., Железов, О.В. (2014). Криптовалюта как феномен современной информационной экономики: проблемы теоретического осмысления. *Интернет-журнал Науковедение*, 24, 5, 1-9.

<sup>2</sup> Бречко, О.В. (2017). Криптовалюта як феномен нової фінансової інфраструктури: проблематика теоретичного осмислення та практичного використання. *Економічний аналіз*, 27, 3, 144-150.