УДК 001+165: 316

**М. В. Онопрієнко**

# ФІЛОСОФСЬКО-МЕТОДОЛОГІЧНІ АСПЕКТИ КРИПТОГРАФІЇ

Інститут досліджень науково-технічного потенціалу
та історії науки імені Г.М. Доброва НАН України
onopriyenko.m@gmail.com

***Анотація.*** *Те, що інформація має цінність, люди усвідомили давно - недарма листування сильних світу цього здавна було об'єктом пильної уваги їх недругів і друзів. Тоді й виникло завдання захисту цього листування від надмірно цікавих очей. Стародавні намагалися використовувати для вирішення цього завдання найрізноманітніші методи, і одним із них був тайнопис – вміння складати повідомлення у такий спосіб, щоб його зміст був недоступним нікому, крім посвячених у таємницю. В наш час інформація набула самостійної комерційної цінності і перетворилася на поширений, майже звичайний товар. Її виробляють, зберігають, транспортують, продають і купують, а значить, – крадуть і підробляють - і, отже, її необхідно захищати. Широке застосування комп'ютерних технологій та постійне збільшення обсягу інформаційних потоків викликає постійне зростання інтересу до криптографії. Пріоритетним завданням криптографії є вдосконалення способів кодування значних масивів інформації, що динамічно оновлюються, змінюючи статус шифрування з активного індивідуального на пасивне масове. Системи захисту шифру корелюють із домінуючими світоглядними парадигмами та напрямами наукової та філософської рефлексії. В сучасному інформаційному просторі переважає інформаційно-образне мислення, виникли нові можливості трансляції, реплікації та діджиталізації знакових систем не тільки у фізичній, але й і у віртуальній реальності. В епоху цифрових комп'ютерних технологій значно розширюється сфера застосування криптографічного кодування як у науково-технічних галузях, так і в широкому контексті людської життєдіяльності (засоби масової інформації, реклама, економічні розрахунки, Інтернет-комунікації, повсякденне життя тощо).*

**Ключові слова:** криптографія, код, знак, шифр, тайнопис, пізнання як творчість, інформація, медіа, віртуальна реальність, безпека даних, інформаційне суспільство.

## Вступ

Уявлення про криптографічні коди має дуже давнє походження, ще з доісторичних часів, коли почав застосовуватися тайнопис у листуванні та різні системи охорони повідомлень. Це сприяло різним формам удосконалення криптографічних систем за рахунок використання математичних та логічних методів. Одночасно криптографія пов'язана з релігійно-езотеричною культурою таїнств, що теж сприяло розвитку її інструментальних засобів.

Сучасний стан науково-технічного розвитку створює попит на поглиблене вивчення феномену криптографії. В інформаційну епоху суспільство зіштовхнулось із важливими проблемами захисту й безпечної трансляції інформації. Розбудова системи криптографічних знаків органічно пов'язана із формами репрезентації смисло-життєвих засад людського буття, сприяючи появі нових варіантів їхніх науково-філософських інтерпретацій. Розвиток технічних засобів персоналізації та ідентифікації створює попит для інновацій, поступово переносячи особистість у віртуальний світ медіа: комунікація в Інтернеті, GRID-мережі, смарт-мережі, брейн-мережі та різноманітні додатки є нічим іншим як трансформацією форм обробки та запису інформації на основі криптографічних кодів.

## Мета та завдання

Метою статті є дослідження філософсько-методологічних аспектів криптографії та розкриття специфіки криптографічного кодування у процесі діджиталізації.

## Методологія дослідження

У наукознавчому дискурсі проблематика розвитку криптографії та безпеки інформаційних даних визріває як значимий об'єкт для дослідження та філософського переосмислення з точки зору методології сучасної науки. Поняття «криптографія», яке традиційно трактувалося у багатьох аспектах, потребує сучасного переосмислення. У філософсько-релігійному аспекті воно означає шифрування та інтерпретацію знаків «священного письма» з метою збереження сокровенності сакрального і водночас адресного донесення та розкриття його потаємного змісту посвяченим в традицію. У філософсько-антропологічному контексті розвиток криптографії відображає зміну світоглядних домінант людського світовідношення і його символічної репрезентації. У семіотичному аспекті криптографія базується на зв'язку між знаком (символом) та його референтами, що дозволяє інтерпретувати значення в площині семіотичного трикутника «знак-об'єкт-сенс». У герменевтичному аспекті передбачає застосування відповідних форм дешифрування, інтерпретації та адекватного розуміння криптографічних кодів.

## Результати досліджень

Мій інтерес до проблем криптографії виник не, як зазвичай, з внутрішніх потреб, а з того, що мене призначили в дисертаційній раді Інституту філософії ім. Г. С. Сковороди НАН України офіційним опонентом кандидатської дисертації А. О. Михальчука «Феномен криптографії в контексті розвитку європейської науки» (Михальчук, 2019) (я професійно займаюсь сучасними мегатехнологіями). Тому що захист дисертації здійнювався за спеціальністю 09.00.09 – філософія науки, головний зміст мого виступу на захисті був присвячений тому, що сучасна філософія науки базується на новій концепції епістемології науки.

Сучасна епістемологія науки трактує пізнання як філософську категорію, що описує процес побудови ідеальних планів діяльності та спілкування, створення знаково-символічних систем. Пізнання – це самостійна реальність, яка пронизує всі аспекти людського світу і лише в абстракції може бути виділена з нього. Стосовно науки пізнання слід розуміти як процес, що супроводжує діяльність і спілкування людей і виконує функцію їхнього забезпечення в ідеальний спосіб. Пізнання – не стільки відображення, скільки має справу із вмістом

колективної діяльності і спілкування, які потребують для своєї організації ідеальних, тобто можливих, пробних, приблизних, варіативних моделей.

Знання як результат пізнання в прямому сенсі виникає з незнання, тобто з інших контекстів досвіду, які потребують знання. Динаміка породження знання носить векторний характер, пов'язана з дослідницькою, пошуковою установкою на розширення сфери ідеальних конструктів.

Шлях пізнання – це рух від стандартних, локальних контекстів досвіду до все більш різноманітних і універсальних, причому чуттєві і розумові елементи присутні на кожному етапі. Функція пізнання полягає в накладанні на світ мережі позначень – наукових формул, моральних норм, художніх образів, магічних символів, що дозволяють людині впорядкувати своє буття в світі і так структурувати свою психіку, щоб надати їй мобільність і варіабельність, забезпечуючи тим самим можливість діяльності та спілкування.

Головна риса людського пізнання, на відміну від аналогічної психіки тварин, – конструктивність. Пізнання не є копіюванням реальності, воно є внесенням сенсу в реальність, створенням ідеальних моделей, що дозволяють спрямовувати діяльність і спілкування і систематизувати акти свідомості. Конструктивна перебудова пізнавальних структур дозволяє здійснювати перехід від одних стандартів людського досвіду до інших, надавати динамічність і творчий характер пізнавальному процесу (Оноприенко, 2019). Це дає можливість розкрити більш ґрунтовно, на сучасному рівні, головні здобутки дисертаційного дослідження.

Це зауваження аж ніяк не відміняло зміст дисертаційного дослідження, навпаки сприяло більш адекватному його аналізу. Дисертація вдало пройшла процедуру захисту і затверджена ДАКом.

В цій статті можна назвати головні риси новизни дисертаційного дослідження А. О. Михальчука.

Криптографія є сукупністю методів кодування/декодування інформації, що забезпечують захист, конфіденційність та аутентифікацію процесів передачі, обробки та зберігання даних. В різні епохи системи криптографічного кодування корелювали із засадничими принципами наукового пізнання. В кожну історичну епоху поставали нові форми і функції криптографії у відповідності до еволюції способів передачі інформації і змін світоглядно-наукової парадигми. В результаті дослідження феномену криптографії виокремлено її основні функції: кодування та захист інформації; збереження, трансляція та реплікація значень; кореляція знаків та знакових систем; інтерпретація знаків; функція заміщення (заміна одних знаково-символічних структур іншими); функція моделювання; функція аутентифікації, діджиталізація (оцифровування криптографічних кодів, їх віртуалізація).

Становлення криптографії пов’язане із появою писемності. В процесі історичної зміни епох та світоглядних систем еволюціонували способи та методи шифрування, змінювалися функції криптографії. В Античності та Середньовіччі її головним завданням було забезпечення сокровенності й незмінності сакральних текстів за допомогою ієрогліфічного та анаграмного шифрування. В епоху Ренесансу традиційні криптографічні способи кодування отримують нові імпульси для трансформації в зв’язку з поширенням ідей гуманізму та антропоцентризму, розширюючи при цьому власні функціональні можливості та соціальну базу застосування; із становленням механістичної картини світу на зміну ручним технологіям шифрування приходять машинні так звані «логічні машини»). У Новий час криптографічні коди отримують, здебільшого, не філософсько-релігійне, а наукове обґрунтування залежно від об'єктно-орієнтованого стилю кодування та емпіричних методів наукового пізнання. В новітню епоху пріоритетним завданням криптографії є вдосконалення способів кодування значних масивів інформації, що динамічно оновлюються, змінюючи статус шифрування з активного індивідуального на пасивне масове.

В процесі історичного розвитку змінюється статус криптографії: в Античності та Середньовіччі криптографія використовується як сукупність методів кодування/декодування для захисту конфіденційних повідомлень та сокровенності сакральних текстів; в період від епохи Відродження до середини XX століття в контексті становлення європейської науки – як сукупність технологічних методів, що використовувалися різними науками та паранауками; із середини XX ст. в період переходу від постіндустріального суспільства до інформаційного криптографія трансформується з технології в галузь дослідження криптології як міждисциплінарної науки, яка складається з криптографії та криптоаналізу на основі синтезу фундаментальної й прикладної математики, фізики (квантової, лазерної, молекулярної, статистичної), лінгвістики, теорії інформації, інформаційної безпеки тощо.

Системи захисту шифру корелюють із домінуючими світоглядними настановами та напрямами наукової та філософської рефлексії. В постіндустріальну добу вплив криптографії яскраво виражений у когнітивних процесах трансформації наукової медіа-інфраструктури. З появою та розвитком квантової науки відбувається становлення нового розділу криптографії – квантової криптографії. Внесення до коду будь-якого числового або лінгвістичного параметру дозволяє розширити спектр можливостей інтерпретації знакових систем, прогнозуючи таким чином нові технологічні виклики науці. Процес кодування/декодування даних на теоретичному та частково на емпіричному рівнях застосовується у процедурах наукового пізнання, формує нові методи роботи з «бітовою» кластерною інформацією і впливає на мислення та світогляд людини, змінюючи у такий спосіб загальну наукову інфраструктуру.

В сучасному інформаційному просторі переважає інформаційно-образне/візуальне мислення. Поняття «криптографії» вийшло за рамки традиційного розуміння специфіки коду як виключно матеріального об’єкта (шифрувального пристрою), отримавши нові можливості трансляції, реплікації та діджиталізації знакових систем не тільки у фізичній, але й і у віртуальній реальності. Інформаційне середовище є частиною реальності у її

різноманітних вимірах (у тому числі, віртуальному). При цьому комбінована реальність, як поєднання фізичної та віртуальної реальності, конструює комфортні умови для існування людини, яка легко може одночасно перебувати у різних вимірах. В цифровому інформаційному гіперпросторі функції реплікації та трансляції інформації дають змогу людині переосмислити онтологічну картину світу, створюючи таким чином не тільки нову синтезовану реальність, а й нові можливості її сприйняття.

В інформаційному суспільстві специфіка кодування зазнала суттєвих змін: моноканальний зв'язок трансформувався в поліканальний, шифрування даних змінило базові принципи та підходи щодо запису інформації (використовуючи сучасні підходи математичних законів аналітичної алгебри та формальної логіки). Криптографія розширила поле наукових досліджень і сферу їхнього практичного застосування, розвиваючи не тільки інформаційне середовище для передачі повідомлень, а й апаратне забезпечення, трансформуючи інформацію від аналогової до цифрової. Базові концепції криптографії відіграють важливу роль у розвитку інформаційного суспільства. Інформаційні знаки та кодові системи стають пріоритетними об’єктами інформаційно-комунікаційної теорії і практики у вимірі сучасної науки (Михальчук, 2019: 16-17).

До цього треба додати ще й такі аргументи: криптографія розширила поле наукових досліджень і сферу практичного застосування, розвиваючи не тільки інформаційне середовище для передачі повідомлень, а й апаратне забезпечення, трансформуючи інформацію від аналогової до цифрової. Процес кодування/декодування даних на різних рівнях визначає зміст наукового пізнання, формує нові методи роботи з «бітовою» кластерною інформацією, її трансляцією та реплікацією в медіа-середовищі, змінюючи характер наукової комунікації. Базові концепції криптографії відіграють важливу роль у розвитку інформаційного суспільства.

В наш час інтенсифікується наукова комунікація завдяки можливостям швидкого обміну значними обсягами інформації та захищеності каналів зв’язку, забезпеченню адресності та конфіденційністі наукової комунікації (Михальчук, 2015; Михальчук, 2017; Михальчук, 2018).

**Обговорення**

Сучасні системи захисту інформації поступово перепрофільовують математичні методи шифрування даних, переходячи від класичного способу кодування даних до квантового. На квантовому типі кодування базується теорія сингулярної послідовності, суть якої: декомпозиція структур – математично-семіотичний метод, який використовує запрограмовану структуру знакових систем з метою подальшої її заміни більш простими підструктурами. У такий спосіб здійснюються мікропроцеси перетворення матричних систем в кванти, що забезпечує зв’язок між підструктурами. Відповідно до трансформації методів кодування змінюються й параметри кореляції між кодами-символами та інструментальними знаками.

Вдосконалення й повсюдне поширення криптографічних систем захисту інформації справляють значний вплив на розвиток науки та інтелектуальних процесів. Розширюються не тільки комунікаційні, але й операційно-технічні можливості наукових досліджень практично у всіх науках – природничих, гуманітарних, технічних. Інтенсифікується наукова комунікація завдяки можливостям швидкого обміну значними обсягами інформації та захищеності каналів зв’язку, забезпеченню адресності та конфіденційності. Збагачується проблематика сучасної філософії науки за рахунок переосмислення традиційного розуміння категорії «реальність» і проблематизації онтологічного статусу віртуальної реальності та криптографічного коду. Слід також відзначити стрімкий розвиток медіафілософії, яка модифікує традиційну філософію техніки, а також зростання інтересу до філософського осмислення проблем безпеки даних і кодування інформації. У постструктуралістській семіотиці зазнала критики структуралістська ідея пошуку метаструктури, універсального метакоду.

Розглядаючи історію криптографії, треба було б головний акцент зробити на драматичних сторінках Першої и Другої світових воєн, змаганні держав у галузі шифрування інформації, виникненні перших логічних та обчислювальних машин. Це б сприяло більш ґрунтовному підходу до наслідків інформатизації суспільства і науки.

**Висновки**

Криптографічні системи корелюють із домінуючими світоглядними парадигмами і напрямами наукової та філософської рефлексії. Сучасні системи захисту інформації поступово перепрофілювали математичні методи шифрування даних, переходячи від класичного способу кодування до квантового. Визначено і проаналізовано функції криптографії в їхній історичній динаміці. В еру цифрових комп'ютерних технологій значно розширюється сфера застосування криптографічного кодування як в науково-технічних областях, так і в широкому контексті людської життєдіяльності (засоби масової інформації, реклама, економічні розрахунки, Інтернет-комунікації, повсякденне життя і так далі). Посилення наукового контексту криптографії сприяє філософському дискурсу про науку як цінність (Башляр, 1987).

**Список літератури**

1. Башляр Г. Научное призвание и душа человека / Г. Башляр // Новый рационализм / Пер. с франц. – М.: Прогресс, 1987. – С. 328-346.

2. Михальчук А. О. Вплив окультизму на розвиток криптографії XV-XVI ст. / А. О. Михальчук // Вісник ХПНУ ім. Г. С. Сковороди «Філософія» «Харк. нац. пед. ун-т ім. Г. С. Сковороди». – Харків: ХНПУ, 2018. – Вип. 50. – С. 115–125.

3. Михальчук А. О. Проблема криптографії: семіотичний аспект / А. О. Михальчук // Збірник наукових праць «Гілея: науковий вісник». – К.: Видавництво «Гілея», 2015. – Вип. 101 (10). – С. 298–300.

4. Михальчук А. О. Системи кодування інформації в античну добу (філософсько-семіотичний аспект) / А. О. Михальчук // «Актуальні проблеми філософії та соціології» «Національний університет «Одеська юридична академія». – Одеса, 2017. – Вип. 18. – С. 90–93.

5. Михальчук А. О. Феномен криптографії в контексті розвитку європейської науки / А. О. Михальчук. – Дис… канд.

філос.наук. 09.00.09 «Філософія науки». – Інститут філософії імені Г. С. Сковороди. – К., 2019. – 26 с.

6. Оноприенко В. И. Методологические ресурсы новой эпистемологии науки / В. И. Оноприенко // Вісник НАУ. Серія: Філософія. Культурологія. – 2019. – № 2 (30). – С. 22-31.

## References

1. Bashlyar, G. (1987). Nauchnoye prizvaniye i dusha cheloveka [Scientific vocation and human soul]: 328-346. Moscow: Progress [in Russian].

2. Mikhalchuk, A. O. (2015). Problema kryptohrafii: semiotychnyi aspekt [The problem of cryptography: a seven-dimensional aspect]. *Zbirnik naukovih prats, Gilea: naukovyy visnik*, 101 (10), 298-300. Kyiv [in Ukrainian].

3. Mikhalchuk, A. O. (2017). Systemy koduvannia informatsii v antychnu dobu (filosofsko-semiotychnyi aspekt) [Systems of codification of information in ancient history (philosophical and semiotic aspects)]. *Aktualni problemy filosofii ta sotsiolohii, Natsionalnyi universytet Odeska yurydychna akademiia*, 18: 90-93. Odessa [in Ukrainian].

4. Mikhalchuk, A. O. (2018). Vplyv okultyzmu na rozvytok kryptohrafii XV-XVI st. [Having infused occultism on the development of cryptography XV-XVI cc.]. *Bulletin of KhPNU im. G.S. Skovorodi "Philosophy",* 50: 115-125. Kharkiv [in Ukrainian].

5. Mykhalchuk, A. O. (2019). Fenomen kryptohrafii v konteksti rozvytku yevropeiskoi nauky [The phenomenon of cryptography in the context of the development of European science]. *Candidate's thesis.* Kyiv [in Ukrainian].

6. Onopriyenko, V. I. (2019). Metodologicheskiye resursy novoy epistemologii nauki[Methodological resources of the new epistemology of science]. *Visnyk Natsionalnoho aviatsiinoho universytetu, Proceedings of the National Aviation University,* 2(30): 22-31 [in Russian].

М. В. ОНОПРИЕНКО

ФИЛОСОФСКО-МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ КРИПТОГРАФИИ

То, что информация имеет ценность, люди осознали очень давно. Недаром переписка сильных мира сего издавна была объектом пристального внимания их недругов и друзей. Тогда-то и возникла задача защиты этой переписки от чрезмерно любопытных глаз. Древние пытались использовать для решения этой задачи самые разнообразные методы, и одним из них была тайнопись – умение составлять сообщения таким образом, чтобы его смысл был недоступен никому, кроме посвященных в тайну. В наше время информация приобрела самостоятельную коммерческую ценность и превратилась в распространенный, почти обычный товар. Ее производят, хранят, транспортируют, продают и покупают, а значит – воруют и подделывают. Следовательно, ее необходимо защищать. Широкое применение компьютерных технологий и постоянное увеличение объема информационных потоков вызывает постоянный рост интереса к криптографии. Приоритетной задачей криптографии является совершенствование способов кодирования значительных массивов информации, которые динамически обновляются, меняя статус шифрования с активного индивидуального на пассивное массовое. Системы защиты шифра коррелируют с доминирующими мировоззренческими парадигмами и направлениями научной и философской рефлексии. В современном информационном пространстве преобладает информационно-образное мышление, возникли новые возможности трансляции, и репликации знаковых систем не только в физической, но и в виртуальной реальности. В эру цифровых компьютерных технологий значительно расширяется сфера применения криптографического кодирования как в научно-технических областях, так и в широком контексте человеческой жизнедеятельности (средства массовой информации, реклама, экономические расчеты, Интернет-коммуникации, повседневную жизнь и т.д.).

*Ключевые слова:* криптография, код, знак, шифр, тайнопись, познания как творчество, информация, СМИ, виртуальная реальность, безопасность данных, информационное общество.

M. Onopriyenko

PHILOSOPHICAL-METHODOLOGICAL ASPECTS OF CRYPTOGRAPHY

**Introduction.** The fact that information has value, people have realized a long time ago. No wonder the correspondence of the high and mighties has long been the object of attention of their foes and friends. It was the time the problem of the protection of that correspondence from the prying eyes arose. The ancients tried to use to solve this problem, a variety of techniques, and one of them was the cipher the ability to compose a message so that its meaning was inaccessible to anyone except the initiated to secrecy. In our time information acquired commercial value and has become widespread, almost a commodity. It is produced, stored, transported, bought and sold, which means - to steal and fake - and therefore it must be protected. Wide application of computer technology and the constant increase in information flows causes a continuous growth of interest in cryptography. **The aim and the tasks.** The priority task of cryptography is the improvement of the ways of encoding significant amounts of information which are dynamically updated, changing the status of the encryption of the active individual on the passive mass. **Research methodology.** System cipher security correlate with dominant ideological paradigms and directions of scientific and philosophical reflection. In the modern information space is dominated by information-creative thinking, new possibilities arose of translation, replication and Djilas sign systems not only in physical but also in virtual reality. **Results of the research.** Reality in its multiple dimensions (including virtual) contains the information environment in which people can be labeled using code that represents her personal data. In this combined reality design a comfortable environment for human existence, which can easily simultaneously be in different dimensions, in particular in the physical dimension of reality and virtuality. This means that the information hyperspace, where the replication and transmission of information enable the person to rethink the ontological picture of the world, thus creating not only a new synthesized reality, but also new possibilities of perception. Today, the code became a subject of interdisciplinary scientific research. Significant changes have occurred in the philosophical and semiotic approaches to its analysis. Discussion. In the information society the value of scientific approaches to the improvement of cryptographic data protection systems will continue to grow. This study provides for the development of this perspective in the following directions: an elaboration of quantum cryptography in the modern information society; signativ aspect of the code in certain areas of operation (media, society, art, science, etc.). **Conclusions.** Cryptographic systems are correlated with the dominant worldview paradigms and directions of scientific and philosophical reflection. Modern information security systems are gradually redefining mathematical methods of data encryption, moving from the classical method of encoding to quantum. The functions of cryptography in their historical dynamics are defined and analyzed. The era of digital computer technology is expanding the scope of cryptographic coding both in the scientific and technical fields and in the broader context of human life (media, advertising, economic calculations, Internet communications, daily life, etc.).

*Key words:* cryptography, code, sign, cipher, mystery, cognition as creativity, information, media, virtual reality, data security, information society.