НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ФІЛОСОФІЇ ІМЕНІ Г. С. СКОВОРОДИ

Михальчук Андрій Олександрович

УДК 003.2 : 26/29 : 167/168

ФЕНОМЕН КРИПТОГРАФІЇ В КОНТЕКСТІ РОЗВИТКУ ЄВРОПЕЙСЬКОЇ НАУКИ

09.00.09 – філософія науки

А В Т О Р Е Ф Е Р А Т
дисертації на здобуття наукового ступеня
кандидата філософських наук

Київ – 2019

Дисертацією є рукопис.

Робота виконана в Східноєвропейському національному університеті імені Лесі Українки, кафедра культурології та хореографічного мистецтва.

Науковий керівник: доктор філософських наук, професор
Головей Вікторія Юріївна,
Східноєвропейський національний університет імені Лесі Українки, завідувач кафедри культурології та хореографічного мистецтва

Офіційні опоненти: доктор філософських наук, професор
Мєлков Юрій Олександрович,
Інститут Вищої освіти Національної академії педагогічних наук України, провідний науковий співробітник

кандидат філософських наук, доцент
Онопрієнко Михайло Валентинович,
Інститут досліджень науково-технічного потенціалу та історії науки імені Г. М. Доброва НАН України, старший науковий співробітник

Захист дисертації відбудеться 27 вересня 2019 р. о 14.00 на засіданні спеціалізованої вченої ради Д 26.161.01 Інституту філософії імені Г. С. Сковороди НАН України за адресою: 01001, м. Київ, вул. Трьохсвятительська, 4.

З дисертацією можна ознайомитися у науковій бібліотеці Інституту філософії імені Г. С. Сковороди НАН України за адресою: 01001, м. Київ, вул. Трьохсвятительська, 4.

Автореферат розіслано 23 серпня 2019 р.

Учений секретар
спеціалізованої вченої ради
доктор філософських наук **Т.В. Гардашук**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність та доцільність теми дослідження. Сучасний стан науково-технічного розвитку створює попит на поглиблене вивчення феномену криптографії (тайнопису). В інформаційну епоху суспільство зіштовхнулось із важливими проблемами захисту й безпечної трансляції інформації. Розбудова системи криптографічних знаків органічно пов'язана із формами репрезентації смисложиттєвих засад людського буття, сприяючи появі нових варіантів їх 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. 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.

Ця проблематика актуальна і в контексті розвитку науково-технічних процесів в сучасній Україні, адже українські науковці свого часу зробили внесок у розвиток криптографії на світовому рівні. Завдяки потужному науковому прориву, здійсненому в науках про інформацію і, зокрема, в кібернетиці під керівництвом академіка В.М. Глушкова, Україна у 60-70-х роках XX ст. була однією з провідних країн у цій галузі, однак із часом, у значні мірі втратила цей науковий потенціал, що суттєво ослабило систему інформаційної безпеки, яка стала вразливою до періодичних масштабних кібератак.

Ключовим для нашого дослідження є поняття «криптографія», яке традиційно трактувалося у багатьох аспектах. 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 відображує 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.

Вагоме значення для методологічного обґрунтування теорії криптографії мали праці відомих філософів, математиків та криптографів, як зарубіжних – Ж. Брассара, М. Вентріса, С. Зінгха, Д. Канна, В. де Касто, О. Кергоффса, Е. Робінсона, К. Розена, В. Стьопіна, П. Торстейнсона, М. Хакена, Дж. Холдена, Е. Хульма, Дж. Чедвіка, Р. Черчхауса, Б. Шнайєра, так і вітчизняних – М. Адаменка, А. Бірюкова, О. Вербіцького, С. Нестерова. Важливими для нашого дослідження стали праці відомих зарубіжних філософів та методологів науки – Т. Куна, К. Поппера, В. Стьопіна, С. Тулміна, П. Фейєрабенда та українських філософів М. Кисельова, В. Лук’янця, О. Мороза, В. Онопрієнка, В. Петрушенка та ін.

У дослідженнях О. Вербіцького, А. Фікса криптографія трактується передусім як важливий фактор безпеки інформаційного суспільства. Дослідниця І. Дуденкова у своїй статті «Філософія як криптографія» аналізує криптографічні стратегії філософії М. Гайдеггера, Ж. Дерріда, К. Мейасу.

Загальнотеоретична специфіка феномену криптографії розкриваються на основі фундаментальних ідей, представлених у текстах філософів античності – Аристотеля, Архімеда, Евкліда, Піфагора, Платона; філософів Середньовіччя – Августина Блаженного, Псевдо-Діонісія Ареопагіта, аль Кінді, Ансельма Кантерберійського, Леонарда Пізанського; мислителів Ренесансу та Нового часу – Ф. Бекона, Леонардо да Вінчі, Й. Кеплера, Г. Лейбніца, Дж. Локка, Л. Пачолі; представників німецької класичної філософії – Г. Гегеля, І. Канта, Й. Фіхте; сучасних філософів – А. Соломоніка, Ж.-П. Сартра, Е. Тофлера, П. Хеменвей; соціологів – Д. Белла, Н. Лумана, М. Кастельса, М. Постера, Т. Рошака; семіологів – У. Еко, В. Іванова, В. Кіма, Ю. Лотмана, Ч. Морріса, Ч. Пірса, Л. Резнікова, Ф. де Соссюра та ін. Важливе значення для дослідження мали наукові доробки філософів, присвячені аналізу особливостей розвитку наукових процесів на основі концепту

постнекласичної раціональності – В. Кізіми, М. Марчука, Ю. Мєлкова, В. Стьопіна, В. Петрушенка та ін.

Філософський аспект аналізу становлення та розвитку криптографії в контексті інформаційної безпеки в Україні висвітлювався на основі праць українських дослідників Є. Архіпової, В. Глушкова, С. Гуфу, О. Дзьобань, М. Журби, Б. Кормича, О. Кулініч, А. Марущака, Л. Павлюк, С. Северина, О. Сороківської, О. Сосніної, присвячених фундаментальним проблемам розвитку інформаційного суспільства.

Аналіз інформаційного суспільства висвітлюється в працях Д. Белла, Н. Віннера, В. Глушкова, В. Лук'янця, Дж. Мартіна, Ю. Мєлкова, Д. фон Неймана, В. Онопрієнка, М. Онопрієнка, Т. Умесао. Аналізом впливу мас-медіа на соціум активно займалися такі теоретики як В. Беньямін, Ж. Бодрійяр, Ж. Дельоз, Р. Ділтс, У. Еко, Н. Луман, М. Кастельс, М. Маклюен, А. Піз, С. Пінкер та ін.

Дослідження «майнінг системи» (криптовалют) як елементу інформаційної безпеки медіа-комунікацій представлені в роботах О. Бречко, Д. Вахрушева, С. Гурцької, Вей Дая, О. Железова, С. Зайцевої.

Аналіз наукової літератури свідчить про те, що зарубіжні та українські дослідники напрацювали значний теоретико-практичний матеріал, який може стати основою для поглибленого філософського переосмислення різноманітних аспектів феномену криптографії в контексті сучасного інформаційного суспільства. Водночас можемо констатувати, що у вітчизняній філософії ще не розроблені проблеми статусу та функцій криптографії в контексті історичного розвитку науки.

Мета дисертації полягає в філософському аналізі теоретико-практичних аспектів становлення криптографії в процесі розвитку європейської науки.

Досягнення поставленої мети передбачає розв'язання таких **завдань**:

- дослідити феномен криптографії та проаналізувати її основні функції в контексті історії європейської науки;
- охарактеризувати історичні витоки європейської криптографічної традиції;

- розробити періодизацію та виявити особливості розвитку криптографії у співвідношенні з етапами становлення і розвитку європейської науки;
- висвітлити теоретико-методологічне підґрунтя дослідження криптографії в контексті проблематики сучасної філософії науки;
- дослідити вплив криптографії на трансформації наукової комунікації;
- проаналізувати особливості сучасних криптографічних систем захисту інформації та їх вплив на розвиток науки та інтелектуальних процесів.

Об'єкт дослідження – феномен криптографії.

Предмет дослідження – криптографічні теорії та практики в контексті розвитку європейської науки.

Теоретично-методологічну основу дисертації утворюють фундаментальні положення та методологічні концепти зарубіжних теоретиків філософії науки – Л. Вітгенштейна, Г. Лейбніца, Т. Куна, П. Фейерабенда, Г. Фреге, Б. Рассела; медіафілософії – В. Беньяміна, Ж. Бодрійяра, Ж. Дельоза, М. Кастельса, Н. Лумана, М. Маклюена та ін. Це передусім концепти «мовних ігор» Л. Вітгенштейна, «симулякрів та симуляції» Ж. Бодрійяра, «міфології знаку» Р. Барта, «ризоми» Ж. Дельоза, «третьої хвилі» Е. Тофлера, теорії «інформаційного суспільства» М. Кастельса, «суспільної комунікації» Н. Лумана, медіа-теорії М. Маклюена та ін. Істотний вплив на дослідження здійснили філософсько-математичні ідеї щодо практичного застосування криптографії (С. Зінгх, Д. Канн, А. Маккей, Д. Маршалл, Е. Хульм); теорія алгоритмів шифрування (М. Адаменко, А. Бірюков, В. Глушков, С. Нестеров, Б. Шнайєр); теорія архітектурної інтерпретації знаку (В. Гропіус, Ч. Дженкс); теорія інтерпретації коду (Е. Робінсон, Дж. Чедвік); теорія комбінаторики та двійкової системи (Дж. Буль, Н. Віннер, Г. Лейбніц); концепт постіндустріального суспільства (Д. Белл, Е. Тофлер); семіотичний аналіз кодів У. Еко; теорія художньо-естетичного кодування Леонардо да Вінчі та ін. У дисертації вищезгадані підходи дозволили розробити методологічний інструментарій філософсько-теоретичного осмислення криптографії на основі міждисциплінарного синтезу (філософії науки, семіотики, медіафілософії,

герменевтики, культурології, теорії інформації) та методологічних принципів, що позиціонуються як засади постнекласичної науки.

Міждисциплінарний підхід дозволяє комплексно проаналізувати соціально-наукові функції криптографії із залученням наукових розробок із галузей філософії, соціології, психології, кібернетики, інформатики, лінгвістики, інженерії. Метод єдності історичного і логічного дозволив виділити основні етапи становлення криптографії в контексті розвитку європейської науки і розробити відповідну періодизацію. Компаративістський підхід дозволив виявити специфіку науково-теоретичного підґрунтя криптографічних систем в різні історичні періоди, а також особливості кодування та декодування інформації в різних медіасередовищах. Застосування герменевтичного методу уможливило інтерпретацію та розуміння криптографічних кодів. Семіотичний метод застосовано в дослідженні знакової природи та структурних особливостей інформаційно-криптографічних систем. Медіафілософський підхід використано при аналізі взаємовпливу медіа-технологій і криптографії.

В методологічному плані для нашого дослідження мають важливе значення доробки вітчизняних дослідників Ю. Генсіцького, А. Єрмоленка, В. Лук'янця, Ю. Мєлкова, О. Мороза, М. Нестерової, В. Онопрієнка, М. Онопрієнка, В. Петрушенка, М. Поповича, О. Рупташ, А. Сторожук, зокрема, стосовно окреслення концепту методологічного плюралізму, оскільки криптографія розглядається нами у різних аспектах як підсистема наукового знання в контексті його соціокультурного побутування.

Наукова новизна одержаних результатів визначається авторським підходом до дослідження та полягає в тому, що вперше здійснено філософський аналіз феномену криптографії в контексті розвитку європейської науки; обґрунтовано, що в кожну історичну епоху поставали нові форми і функції криптографії у відповідності до еволюції способів передачі інформації і змін світоглядних настанов та досягнень науки. Криптографію концептуалізовано як поліфункціональний феномен, пріоритетними функціями якого є: кодування та декодування інформації як наріжного елементу комунікації загалом, та наукової комунікації зокрема;

збереження, трансляція та реплікація значень; кореляція знаків та знакових систем; інтерпретація знаків; функція заміщення та моделювання. На підставі теоретичного аналізу проблеми здобуто й обґрунтовано низку узагальнень та положень, що мають наукову новизну і виносяться на захист:

Вперше:

– обґрунтовується, що в процесі історичного розвитку змінюється статус криптографії: в античності та Середньовіччі криптографія використовувалася як сукупність технологій кодування/декодування для захисту конфіденційних повідомлень та сокровенності сакральних текстів; в період від епохи Відродження до сер. XX ст. – як сукупність науково-технологічних методів, що використовувалися різними науками та паранауками; з сер. XX ст. зі становленням інформаційного суспільства криптографія трансформується з рівня технології у міждисциплінарну науку криптологію;

– доведено, що принципи криптографічного кодування/декодування даних на різних рівнях є вагомою складовою сучасного наукового пізнання, формуючи нові математично-лінгвістичні методи роботи з кластерною інформацією, що характеризуються переходом від апаратних до програмних систем із застосуванням прикладної математики і лінгвістики, кібернетики, оптики, інформатики, диференціації штучних мов програмування, що сприяє суттєвому прискоренню трансляції й реплікації інформації в медіа-середовищі та інтенсифікації наукової комунікації;

– сформульовано базові принципи теорії сингулярної послідовності, в основі якого є математично-семіотичний метод, який використовує запрограмовану структуру знакових систем з метою подальшої її заміни більш простими підструктурами. Таким чином здійснюються мікропроцеси перетворення матричних (знакових) систем в кванти, що забезпечує зв’язок між підструктурами; відповідно до трансформації методів кодування змінюються й параметри кореляції понять між кодовими знаками та знаками інструментальними: кодові знаки (які задають алгоритм упорядкування, наприклад математичної формули) та знаками інструментальними (які підпорядковуються кодовим знакам, наприклад окремого

елементу цієї формули, що втрачає свої властивості, якщо її розглядати в одиночній площині);

– обґрунтовано положення про те, що вдосконалення й повсюдне поширення криптографічних систем захисту інформації мають значний вплив на розвиток науки та інтелектуальних процесів: розширюються не тільки комунікаційні, але й операційно-технічні можливості наукових досліджень – природничих, гуманітарних, технічних; інтенсифікується наукова комунікація завдяки можливостям швидкого обміну значними обсягами інформації та захищеності каналів зв'язку, забезпеченню адресності та конфіденційності;

– розробка криптографічних систем масиву інформаційних даних «Big-Data» закладає тенденцію переходу суспільства від цифрової ери до квантової; філософсько-математична система Г. Лейбніца, в основі якої закладено формулу двійкової системи «0 та 1», змінюється на нову «кубітну» систему квантових комп'ютерів, що уможливлює реалізацію квантових процесів інформатизації науки та суспільства; відбувається зміна наукової картини світу (одні засадничі структури, зокрема атоми, змінюються на інші, зокрема кванти, кубіти), збагачується проблематика сучасної філософії науки за рахунок переосмислення традиційного розуміння категорії «реальність» і проблематизації онтологічного статусу віртуальної реальності та криптографічного коду.

Уточнено:

– дефініцію поняття «криптографія», яку ми визначаємо як сукупність методів кодування/декодування інформації, що забезпечують захист та конфіденційність процесів передачі, обробки та зберігання даних; криптографія розглядається як предмет міждисциплінарної галузі дослідження криптології;

– особливості інформаційних кодів як важливих елементів наукової комунікації, значимість якого проявляється в науково-методологічній рефлексії, специфіку кодування інформації в комунікаціях мас-медіа.

Отримали подальший розвиток:

– концепт «інформаційного суспільства», який застосовується для визначення статусу когнітивних процесів мислення людини у вимірі мас-медіа, на основі якого

сформувалося нове філософське осмислення поняття «інформаційної безпеки», що було пов’язано з історичним розвитком шифру та криптографії в цілому.

Науково-практичне значення одержаних результатів полягає в тому, що філософський аналіз феномену криптографії в контексті розвитку науки виводить дану проблему на новий рівень наукового розгляду. Одержані результати дисертаційного дослідження можуть бути використані як методологічні засади для подальшого аналізу криптографії та пошуку нових філософських і культурологічних підходів до її розуміння. Здобуті висновки дозволяють досліджувати практичну криптографію як філософське явище, поновлюючи аналіз проблем, неоднозначних феноменів, теорій та тенденцій у сучасній науці. Положення та висновки, отримані в результаті дослідження, також можуть використовуватися під час викладання курсів із філософії науки, філософії культури; спецкурсів із безпеки інформації й масової комунікації, медіафілософії та інших дисциплін.

Апробація результатів дослідження здійснювалася шляхом оприлюднення основних положень і висновків дослідження, виступів та доповідей на 3 (трьох) міжнародних науково-практичних конференціях: Міжнародній науково-практичній конференції «Сучасні виклики для суспільних наук в умовах глобалізації» (м. Львів, 29-30 травня 2015р.); Міжнародній науково-практичній конференції «Суспільні науки: напрями та тенденції розвитку в Україні та світі» (м. Одеса, 17-18 липня 2015р.); VII Міжнародній науковій конференції «New achievements of world science» (США, м. Морісвіль, 22-23 червня 2017р.).

Публікації. Результати дослідження висвітлено у 8 (восьми) наукових працях, 4 з яких опубліковані у фахових виданнях України і 1 стаття – у періодичному закордонному виданні, внесеному до міжнародних науково-метричних баз, 3 − тези доповідей на міжнародних науково-практичних конференціях.

Структура дисертації визначена логікою розкриття досліджуваної теми. Робота складається з вступу, трьох розділів (дев'яти підрозділів), висновків до них, загальних висновків та списку використаних джерел із 314 найменувань та 8 додатків. Повний обсяг дисертації складає 228 сторінки, з яких основний текст дисертації викладений на 196 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У «Вступі» обґрунтовано актуальність теми дисертації, сформульовано мету й завдання дослідження, визначено його об'єкт та предмет, розкрито теоретико-методологічні засади та наукова новизна роботи, окреслено теоретичне й практичне значення дисертації, подано інформацію про її апробацію та структуру.

У першому розділі «Теоретико-методологічне підґрунтя дослідження» розкривається зміст ключових понять криптографії (символу, коду, знаку, образу), аналізуються теоретико-методологічні підходи до осмислення поняття «код» та його похідні концепти.

Підрозділ 1.1. «Аналіз джерел та наукових публікацій із досліджуваної проблематики» присвячений систематизації джерел та філософських теорій, які дотичні до філософського осмислення проблематики криптографії. Проаналізовано витоки концепту знакового коду в прагматичній філософії Ч. Пірса, лінгвістичній концепції Ф. де Соссюра, семіозису Ч. Морріса, математичних концепціях криптографії Д. Чедвіка, С. Зінгха та Д. Канна, які знайшли своє продовження у сучасній філософії науки.

Рівень знань про взаємозв’язки між різноманітними логічними знаково-символьними структурами є своєрідним гносеологічним маркером розвитку інформаційного суспільства та технологій. Зміна площини досліджуваної проблематики дозволяє переосмислити базові концепти криптографії з точки зору структуралізму, герменевтики та теорії інформації. Аналіз джерел та наукової літератури засвідчує, що зарубіжні дослідники активно розробляють як практичний, так і категоріально-поняттєвий аспекти криптографії, у той час як в Україні філософсько-методологічний аспект цього феномену до сьогодні не розроблений.

У п*ідрозділі 1.2. «Категоріально-поняттєвий апарат дослідження феномена криптографії»* висвітлюється криптографічний підхід до тлумачення природи знака в епоху «наукового прориву» в XVI-XVII ст. (Б. де Віженер, Г. Лейбніц, Дж. де ла Порта); концепт езотеричної природи коду як атрибуту знаково-символьних взаємозв'язків (Ф. Гогенхайм, А. Неттесгеймський, П. Хеменвей); семіотичне тлумачення коду як основи комунікативної рефлексії (Р. Барт, У. Еко, Ч. Морріс,

Ч. Пірс, Ф. де Соссюр); концепт «мовних ігор» Л. Вітгенштейна; кодування комунікацій на рівні функціональних підсистем суспільства (Е. Кастельс, Н. Луман); осмислення специфіки архітектурного коду (В. Гропіус, У. Еко, Ч. Дженкс); герменевтичне значення коду в контексті фундаментальних антропологічно-екзистенційних змін в понятті інформаційного суспільства (Д. Белл, Ж. Бодрійяр, Ж. Дельоз); концепт «Третьої хвилі» Е. Тоффлера, у якому код розглядається як когнітивно-комунікативний чинник сучасного неоінформаційного суспільства тощо.

Розглядаються філософсько-герменевтичний та семіотичний підходи до осмислення феномену криптографії, що вплинули на формування категоріально-понятєвого апарату дослідження. Аналізуються низка ключових для нашого дослідження понять («криптографія», «криптологія», «криптоаналіз», «код», «знак», «символ», «криптограма», «стеганограма» та ін.) та концептів («ризома», «аура», «симулякри та симуляція», «мовні ігри», «третя хвиля» тощо).

Шифр осмислюється як логічна побудова взаємозв'язків між знаками, оскільки кожний знак несе в собі приховане значення, яке може змінюватися в залежності від об'єктно-орієнтованого стилю кодування та емпіричних методів наукового пізнання. Ці поняття та методологічні підходи формують методологічне підґрунтя для філософського переосмислення криптографічної проблематики в контексті розвитку європейської науки.

У другому розділі «Основні етапи розвитку криптографічної традиції в контексті становлення європейської науки» прослідковується еволюція ідеї кодування інформації за допомогою численних криптографічних систем та їх зв’язок з європейськими філософськими течіями та герменевтично-езотеричними традиціями.

Підрозділ 2.1. «Криптографія в епоху античності» присвячений дослідженню особливостей криптографічних систем в епоху античності. Уточнено низку таких концептуальних понять дискурсу криптографії як «шифр», «шифрувальний пристрій», «код», «символ», «філософія кодування», «золотий перетин».

Показано, що в епоху античності системи кодування (наприклад анаграмне кодування) корелюються з ідеями наукового пізнання, на основі яких пізніше

відбувається становлення європейської науки. У цей період комплекс питань, пов'язаних з вивченням коду, має філософсько-математичне та герменевтичне підґрунтя (Аристотель, Евклід, Піфагор, Плутарх, Птолемей, Філон). Розуміння криптографічного знаку (аудіального, візуального) як певної матеріально-ідеальної структури корелюється із позицією класичного монізму – однієї істини, до якої може привести лише один істинний метод. Таким чином знак виражає одну істину, оскільки «абсолютний» істинний метод здатний набувати властивостей шифру кодування даних, змінюючи форму запису з метою збереження важливої інформації.

Підрозділ 2.2. «Теорія і практика криптографії в добу Середніх Віків» присвячений аналізу особливостей розвитку криптографії доби європейського Середньовіччя в контексті домінування теоцентричної ідеології.

У середньовічному богословсько-теологічному дискурсі знаковий символізм набуває нового сакрально-гносеологічного відтінку. Для філософсько-теологічної екзегетики важливе методологічне значення мали ідеї Августина Блаженого, Роджера Бекона, Ансельма Кантерберійського, Псевдо-Діонісія Ареопагіта, Фоми Аквінського, та ін., в основі яких лежали два ключових компонента: матеріальна природа знаку (відтворення знаку в матеріальному світі) та містична природа знаку (духовне споглядання образів Божественного, трансцендентного).

В цю добу розвиток криптографії інспірується, здебільшого, філософсько-релігійними течіями. Проаналізовано особливості розвитку герменевтичного та семіотичного аспектів криптографії в середовищі представників патристики (Августин Блажений, Псевдо-Діонісій Ареопагіт), кабалістики (Авраам Абулафія), філософів-схоластів (Августин Блажений, Ансельм Кантерберійський, Фома Аквінський, Дунс Скот) та представників середньовічних релігійних орденів (Роджер Бекон, Раймонд Луллій). Їх зусиллями були реорганізовані структурні принципи криптографії, криптографічні коди співвідносилися з езотеричними символами зв’язку видимого та невидимого, людського й Божественного. Таким чином таємне знання набувало репрезентативного характеру, відтворюючи в текстах зашифровані повідомлення та закладаючи підґрунтя для нової картини світу.

Підрозділ 2.3. «Криптографічні системи епохи Ренесансу» присвячений аналізу криптографічних систем та кодів цього періоду.

В епоху Ренесансу вперше концептуалізується поняття криптографії (Іоанн Тритемій), розширюється сфера її використання як в релігійних, окультних, так і наукових трактатах, а також у дипломатичній та економічній діяльності, тобто в публічному секторі. Значна кількість наукових, мистецьких, соціальних, філософських, релігійних, політичних ідей репрезентувалися у зашифрованому вигляді, що було обумовлено потребою захисту від переслідувань інквізиції, цензури контрреформації, швидкозмінної політичної кон'юнктури тощо. Акцент в таких текстах переносився з сакрального змісту на акт свідомого сприйняття, розуміння та інтерпретації. Криптографія цієї епохи тісно пов'язана із контекстом становлення європейської науки, із поступовою секуляризацією свідомості й автономізацією людського інтелекту. Із становленням механістичної картини світу на зміну ручним технологіям шифрування приходять машинні пристрої (т.зв. «логічні машини»).

Криптографічні способи кодування (текстовий, числовий, звуковий, пікторальний) отримують нові імпульси для трансформації в зв'язку з поширенням механістичної системи знання, ідей гуманізму та антропоцентризму, розширюючи при цьому власні функціональні можливості та соціальну базу. Філософсько-наукові ідеї Дж. Бруно, Леонардо да Вінчі, Й. Кеплера, Миколи Кузанського сприяли розробленню нових способів та інструментарію технології шифрування.

Підрозділ 2.4. «Криптографія Нового часу та новітньої епохи» присвячений проблемі трансформації методології шифрування під впливом створення базових понять комбінаторики (Ф. Бекон, Г. Галілей, Р. Декарт, Г. Лейбніц). Завдяки науковим методам пізнання та філософським ідеям Нового часу (Дж. Берклі, Г. Гегеля, Т. Гоббса, І. Канта, Й. Фіхте) криптографія отримує новий поштовх у своєму розвитку. В класичній науці код отримує своє чітке концептуальне значення в герменевтичному і семіотичному аспектах, зокрема, в контексті збереження та відтворення знання. У добу Нового часу криптографічні коди отримують,

здебільшого, не філософсько-релігійне, а наукове обґрунтування в залежності від об'єктно-орієнтованого стилю кодування та емпіричних методів наукового пізнання.

У кінці XIX – першій половині XX ст. завдяки гіпотетико-дедукційному та формалізаційному методам побудови наукових теорій криптографія набуває нового осмислення в контексті трансформації від модерної до сучасної науки. Розвиток семіотики, зокрема теорії знаку Ч. Пірса, Ч. Морріса, лінгвістичної семіології Ф. де Соссюра, сприяли становленню категоріально-поняттєвого апарату теорії та практики криптографії.

З появою аналітичних, а пізніше електро-обчислювальних машин розширюється сфера застосування криптографії в контексті і соціогуманітарної, і науково-технологічної сфери, що сприяло зародженню теорії інформації, складовою частиною якої стає криптоаналіз.

Третій розділ *«Криптографічні коди в інформаційному науково-технічному просторі»* розкриває специфіку криптографії та її значення у формуванні засад комунікативних процесів постіндустріального інформаційного суспільства. Зосереджено увагу на семіотичному та інформаційному аспектах концепту безпеки даних в сучасному цифровому вимірі в умовах поширення даних через новітні комунікаційні мережі.

Підрозділ 3.1. «Специфіка кодування в інформаційному суспільстві» присвячений аналізу тенденцій розвитку систем кодування в інформаційному суспільстві та зростанню їх ролі у вимірі аналогово-цифрових технологій. З'ясовано форми комунікації, що забезпечують функціональні можливості безпечної трансляції даних в інформаційному суспільстві (цілісність, конфіденційність та аутентичність). Одним із рушійних факторів переходу від модерної до сучасної науки є запровадження нових парадигмальних наукових концептів інформації та інформаційних технологій, що стимулює формування нової картини світу, в якій домінують нелінійність, стохастичність, ризоматичність. Конвергенція науки та інформатики призводить до суттєвих змін в науковій та соціальній сферах життя. Сформульовано теорію сингулярної послідовності, в основі якого лежить аксіоматична ідея кореляції між кодовими знаками і знаками інструментальними.

Обґрунтовується, що в сучасній криптографії реалізується міждисциплінарний синтез фундаментальних наук, прикладних наук (оптики, механіки, прикладної математики), інженерії, формальної логіки, теорії інформації тощо. Цей синтез передбачає рівень не тільки визначення самого коду (знака) та його алгоритму (функції передачі / отримання повідомлень), але й рівень процесу шифрування цих повідомлень відповідно до функцій та цілей масиву даних («Big-Data»).

У п*ідрозділі 3.2. «Семіотичний аналіз криптографічних кодів в Інтернет-комунікаціях» д*осліджуються сучасні алгоритми безпеки даних під час використання процедури комунікації в глобальній мережі Інтернет. Охарактеризовано поняття криптовалюти як семіотичного криптографічного коду, що виконує роль віртуальних операцій в інформаційному суспільстві шляхом процесу анігіляції. Аналізуються причини зростання ролі систем безпеки даних (безпека трансляції повідомлення в епоху науково-технологічного буму, інтенсифікація наукової комунікації, розгалуження апаратних комплексних систем, наприклад серверів тощо), що набуває важливого статусу – не тільки технологічного, але й наукового. Здійснено філософсько-семіотичний аналіз коду як адаптивної безпекової платформи, що активно взаємодіє з різними сферами науки та техніки. Зазначається, що у постструктуралістській семіотиці зазнала критики структуралістська ідея пошуку мета-структури («структури структур»), універсального мета-коду. Натомість в еру комп'ютерних технологій експлікація поняття коду переноситься з метафізичного й онтологічного вимірів у онтичний вимір – у широкий контекст людської життєдіяльності (засоби масової інформації, мода, реклама, Інтернет-комунікації, повсякденне життя тощо).

У *підрозділі 3.3. «Вплив систем захисту інформації на розвиток науки та людського інтелекту»* досліджуються різноманітні форми такого впливу у технічному, мовному та психолінгвістичному аспектах. Технічний аспект характеризується динамікою розвитку сучасного програмного забезпечення, трансформуючи процес «живої» комунікації у віртуальне середовище. Прискорене вдосконалення технічних гаджетів із модернізованими криптографічними системами захисту вимагає нових інтелектуальних навичок та стимулює розвиток

конкуренції у сфері розробки нових технологій, а отже – розвиток наукового потенціалу, розширюючи міждисциплінарні зв’язки між різними секторами наукової діяльності. Аналіз мовного аспекту виявив сучасні тенденції розробки знаково-кодових систем вербальної та невербальної мови, що закладають фундамент для створення нових штучних мов програмування. Проаналізовано значення нейролінгвістичних практик кодування свідомості для розробок штучного інтелекту та сучасних технологій нейролінгвістичного впливу, що можуть мати маніпулятивний характер. Зменшенню негативних наслідків такого впливу сприятиме створення розгалуженої системи медіаосвіти, формування критичного мислення, т.зв. «інформаційного імунітету». Важливим чинником ефективного розвитку цієї системи є вдосконалення алгоритмів криптографічного кодування, що забезпечує захищеність каналів трансляції інформації, її конфіденційність.

ВИСНОВКИ

За підсумками виконаного дисертаційного дослідження у відповідності до поставленої мети та завдань зроблено такі **висновки:**

1. 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 корелювались 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).

2. 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 пристрої (т.зв. «логічні машини»). У добу Нового часу криптографічні коди отримують, здебільшого, не філософсько-релігійне, а наукове обґрунтування в залежності 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 сер. XX століття в контексті становлення європейської науки – як сукупність технологічних методів, що використовувалися різними науками та паранауками; з сер. XX ст. в період переходу від постіндустріального суспільства до інформаційного криптографія трансформується з технології в галузь дослідження криптологію як міждисциплінарну науку, яка складається з криптографії та криптоаналізу на основі синтезу фундаментальної й прикладної математики, фізики (квантової, лазерної, молекулярної, статистичної), лінгвістики, теорії інформації, інформаційної безпеки тощо.

3. Виявлено, що системи захисту шифру корелюються із домінуючими світоглядними настановами та напрямами наукової та філософської рефлексії. В постіндустріальну добу вплив криптографії яскраво виражений у когнітивних процесах трансформації наукової медіаінфраструктури. 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 таким чином загальну наукову інфраструктуру.

4. Доведено, що в сучасному інформаційному просторі переважає інформаційно-образне/візуальне мислення. Поняття «криптографії» вийшло за рамки традиційного розуміння специфіки коду як виключно матеріального об’єкту (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.

5. 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 їх 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.

6. 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. Таким чином 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.

7. 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 мета-структури, універсального мета-коду. Натомість в еру 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).

8. В інформаційному суспільстві значення наукових підходів до вдосконалення криптографічних систем захисту даних будуть надалі зростати та розвиватимуться в наступних напрямках: проблема квантової криптографії, що актуалізується в умовах розвитку сучасного інформаційного суспільства; сигнітивний аспект коду в окремих сферах його функціонування (медіа, соціум, мистецтво, науки тощо).

СПИСОК ПРАЦЬ, ОПУБЛІКОВАНИХ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України:

1. 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.

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

3. 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.

4. Михальчук А. О. Стилі кодування та їх вплив на інтелект людини в контексті сучасного інформаційного суспільства / А. О. Михальчук // Збірник наукових праць «Гілея: науковий вісник». – К.: Видавництво «Гілея», 2018. – Вип. 137. – С. 207–211.

Статті у закордонних наукових фахових виданнях:

5. Михальчук А. О. Криптографічні коди у контексті сучасної медіа-культурної діяльності / Михальчук А. О. // Європейський філософський та історичний дискурс. – Прага, 2018. – Том 4. – Вип. 2. – С. 114–119.

Матеріали науково-практичних конференцій

6. Михальчук А. О. Проблема криптографії: семіотичний аспект / А. О. Михальчук // Сучасні виклики для суспільних наук в умовах глобалізації: Матеріали міжнародної науково-практичної конференції, Львів, 29–30 травня 2015 р.: тези доповіді. – Львів: ГО «Львівська фундація суспільних наук», 2015. – С. 28–30.

7. Михальчук А. О. Поняття криптографії в епоху античності / А. О. Михальчук // Суспільні науки: напрямки та тенденції розвитку в Україні та світі: М-ли міжн. науково-практичної конференції, Одеса, 17–18 липня 2015 р.: тези доповіді. – Одеса: ГО «Причорноморський центр досліджень проблеми суспільства», 2015. – С. 80–82.

8. Mykhalchuk A. Symbolic «Divine Proportion» in ancient Cryptography / Proceedings of VII International scientific conference «New achievements of world science». – Morrisville, Lulu Press., 2017. – P. 50–54. [in Ukrainian].

АНОТАЦІЇ

Михальчук А. О. Феномен криптографії в контексті розвитку європейської науки. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата філософських наук за спеціальністю 09.00.09 «Філософія науки». – Інститут філософії імені Г. С. Сковороди. – Київ, 2019.

Дисертація присвячена філософському аналізу теоретико-практичних аспектів становлення криптографії в контексті розвитку європейської науки. Розроблено періодизацію та виявлено особливості конкретних етапів історичного розвитку криптографії у співвідношенні з етапами становлення європейської науки. Визначені та проаналізовані функції криптографії в їх історичній динаміці. Виявлено, що криптографічні системи корелюються із домінуючими світоглядними парадигмами та напрямами наукової та філософської рефлексії. Доведено, що сучасні системи захисту інформації поступово перепрофільовують математичні методи шифрування даних, переходячи від класичного способу кодування до

квантового. Обґрунтовано, що в еру 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, інформація, медіа, віртуальна реальність, безпека даних, інформаційне суспільство.

Михальчук А. А. Феномен криптографии в контексте развития европейской науки. Квалификационная научная работа на правах рукописи.

Диссертация на соискание ученой степени кандидата философских наук по специальности 09.00.09 «Философия науки». – Институт философии имени Г. С. Сковороды. – Киев, 2019.

Диссертация посвящена философскому анализу теоретико-практических аспектов становления криптографии в контексте развития европейской науки. Концептуализовано теоретико-методологическое основание исследования криптографии. Разработана периодизация и выявлены особенности конкретных этапов исторического развития криптографии в соотношении с этапами становления европейской науки. Определены и проанализированы функции криптографии в их исторической динамике.

Выявлено, что криптографические системы коррелируются с доминирующими мировоззренческими парадигмами и направлениями научной и философской рефлексии. Процесс кодирования / декодирования данных на теоретическом и частично на эмпирическом уровнях применяется в процедурах научного познания, формирует новые методы работы с «битовой» кластерной информацией и влияет на мышление и мировоззрение человека, изменяя таким образом научную инфраструктуру. Обосновано, что понятие криптографического кодирования вышло за рамки его традиционного понимания, чему способствовали новые возможности трансляции, репликации и диджитализации криптографических знаков не только в физической, но и в виртуальной реальности.

Обосновано, что информационное общество динамически развивается в эпоху цифровых технологий. С развитием компьютерных технологий значение принципов криптографического кодирования, как и влияние информации на интеллект человека, возрастает экспоненциально. Медиа-коммуникации постепенно заменяют привычное общение, трансформируя процессы мышления и деятельности человека в направлении от реального к виртуальному. Реальное измерение является сферой нелинейного научного познания; а виртуальное – проекцией новой цифровой реальности, и в нем преобладает не абстрактное, а интегративно-технологическое мышление.

Доказано, что современные системы защиты информации постепенно перепрофилируют математические методы шифрования данных, переходя от классического способа кодирования к квантовому. Утверждается, что с появлением и развитием квантовой науки происходит становление нового раздела криптографии – квантовой криптографии. Интенсифицируется научная коммуникация благодаря возможностям быстрого обмена большими объемами информации и защищенности каналов связи, обеспечению адресности и конфиденциальности. Обосновано, что 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, повседневная жизнь и т.д.).

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

Mykhalchuk A. The phenomenon of cryptography in the context of the development of European science. – Manuscript.

Dissertation for the degree of candidate of philosophical sciences, specialty 09.00.09 «Philosophy of science». – H. Skovoroda Institute of Philosophy, National Academy of Sciences of Ukraine. – Kyiv, 2019.

The dissertation is devoted to the philosophical analysis of theoretical and practical aspects of the formation of cryptography in the context of the development of European science. Proposing the periodization, we have identified the features of specific stages of the historical development of cryptography in relation to the stages of formation and development of European science. The functions of cryptography in their historical dynamics are determined and analyzed.

The cryptographic systems correlate with dominant ideological paradigms and directions of scientific and philosophical reflection. It is proved that modern information security systems gradually rephrase the mathematical methods of encrypting data and move from the classical method of encoding to quantum. It is substantiated that the sphere of digital computer technologies significantly expands the scope of cryptographic encoding both in scientific and technical fields and in the broad context of human activity (media, advertising, economic calculations, Internet communications, everyday life etc.).

Key words: cryptography, code, sign, cipher, secret, information, mass media, virtual reality, data security, information society.

Підписано до друку 21.08.2019 р. Формат 60х84 1/16. Папір офсетний.
Друк на різографі. Обсяг 0,9 ум. друк. арк. 0,9 обл.-вид. арк.
Наклад 100 пр. Зам. 85. Виготовлювач – Вежа-Друк
(м. Луцьк, вул. Шопена, 12, тел. (0332) 29-90-65).