В І Д Г У К

кандидата філософських наук, старшого наукового співробітника Державної установи «Інститут досліджень науково-технічного потенціалу та історії науки ім. Г.М. Доброва НАН України» *Онопрієнка Михайла Валентиновича* на дисертацію *Михальчука Андрія Олександровича «ФЕНОМЕНКРИПТОГРАФІЇ В КОНТЕКСТІ РОЗВИТКУ ЄВРОПЕЙСЬКОЇ НАУКИ»,* що подана у спеціалізовану раду Д. 26.161.01 в Інституті філософії імені Г.С. Сковороди НАН України на здобуття наукового ступеню кандидата філософських наук за спеціальністю 09.00.09 - філософія науки

Те, шо інформація має цінність, люди усвідомили дуже давно - недарма листування сильних світу цього здавна було об'єктом пильної уваги їх недругів і друзів. Тоді-то і виникла задача захисту цього листування від надмірно цікавих очей. Стародавні намагалися використовувати для вирішення цього завдання найрізноманітніші методи, і одним з них був тайнопис - вміння складати повідомл'ення таким чином, щоб його зміст був недоступний нікому, крім посвячених у таємницю. Є свідоцтва того, що мистецтво тайнопису зародилося ще в доантичні часи.

В наш час інформація прид іала самостійну комерційну цінність і перетворилася на широко 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. Останнім часом збільшується роль програмних засобів захисту інформації, які не потребують великих фінансових витрат у порівнянні з апаратними криптосистемами. Сучасні методи шифрування гарантують практично абсолютний захист даних.

ТСриптологія - це наука про пеі створення інформації для забезпечення її секретності, що складається з двох гілок: криптографії та криптоаналізу. *Криптографія* - наука про способи перетворення (шифрування) інформації з

метою її захисту від незаконних користувачів. Історично першим завданням криптографії був захист переданих текстових повідомлень від несанкціонованого ознайомлення з їх змістом, відомого тільки відправнику і одержувачу, всі методи шифрування є лише розвитком цієї філософської ідеї, з ускладненням інформаційних взаємодій в людському суспільстві виникли і продовжують виникати нові завдання по їх захисту, деякі з них були вирішені в рамках криптографії, що зажадало розвитку нових підходів і методів.

До здобутків дисертаційного дослідження треба віднести виокремлення і обгрунтування великої наукової проблеми криптографії з широким філософсько-методологічним контекстом. Це зроблено вперше в Україні. Проблема криптографії має значні перспективи і потребує зусиль колективів дослідників.

У дисертації відмічається, що в новітню епоху пріоритетним завданням криптографії є вдосконалення способ .в 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.

Доведено, що в сучасному інформаційному просторі переважає інформаційно-образне мислення. Поняття «криптографії» вийшло за класичні рамки античного розуміння специфіки коду як виключно матеріального предмету (шифрувального пристрою), отримавши нові можливості трансляції, реплікації та діджиталізації знакових систем н(тільки у фізичній, але й і у віртуапьній реальності. Зазначається, що реальність у її різноманітних вимірах (у тому числі, віртуальному) містить інформаційне середовище, в якому людина може бути означена за допомогою коду, що репрезентує Гї персональні дані. При цьому комбінована реальність конструює комфортні умови для існування людини, яка легко може одночасно перебувати у різних вимірах, зокрема, у вимірі фізичної дійсності й віртуальності. Це означає, що інформаційний гіперпростір, у якому

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.

У сучасному інформатизованому світі криптографія стає все більше затребуваною, зростають її значення та вплив на різноманітні процеси у сферах науки, техніки, економіки, політики та суспільства в цілому. Сьогодні код став багатогранним предметом міждисциплінарних наукових досліджень. Суттєві зміни відбулися у філософсько-семіотичних підходах до його аналізу. У постструктуралізмі зазнала критикк 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 оптичний вимір - у широкий контекст людської життєдіяльності (засоби масової інформації, мода, реклама, Інтернет-комунікації, повсякденне життя тоїцо).

В інформаційному суспільстві специфіка кодування зазнала суттєвих змін: моноканальний зв'язок трансформувався в поліканальний, шифрування даних змінило базові принципи та підходи пі;одо запису інформації (використовуючи сучасні підходи математичних закс нів аналітичної алгебри та формальної логіки). 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-середовиїці, змінюючи характер наукової комунікації. Базові концепції криптографії відіграють важливу роль у розвитку інформаційного суспільства. Інформаційні знаки та кодові системи стають ріоритетними об'єктами інформаційно-комунікаційної теорії і практики у вимірі постнекласичної науки.

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

Обіґрунтовано, що вдосконалення й повсюдне поширення криптографічних систем захисту інформації мають значний вплив на розвиток науки та інтелектуальних процесів. Розширюються не тільки комунікаційні, але й операційні технічні можливості іаукових досліджень - природничих, гуманітарних, технічних. Інтенсифікується наукова комунікація завдяки можливостям швидкого обміну значними обсягами інформації та захиіценості каналів зв'язку, забезпеченню адресності та конфіденційністі наукової комунікації.

Стверджується, іцо в інформаційному суспільстві значення наукових підходів до вдосконалення криптографічних систем захисту даних будуть надалі зростати. Дане дослідження передбачає розвиток цієї проблематики в наступних напрямках: проблема квантової криптографії, іцо актуалізується в умовах розвитку сучасного інформаційного суспільства; сигнітивний аспект коду в окремих сферах його функціонування (медіа, соціум, мистецтво, науки тощо). Дослідження вказаної проблематики на основі розроблених у роботі положень відкривають нові перспективи для подальшого вивчення феномену криптографії в контексті сучасної філософії науки.

Зауеаэюення до тексту дисертації торкаються деяких принципових проблем.

Останнім часом філософія на пострадянському просторі нарешті позбулася наслідків теорії відображення. Пізнання і свідомість розуміються в межах цієї концепції як відображення. Відтворення характеристик предметів, які існують об'єктивно, реально, незалежно від свідомості суб'єкта. Сам термін «відображення» є досить невдалим, оскільки викликає уявлення про пізнання як наслідок причинного впливу реального предмета на пасивного суб'єкта, що сприймає цей вплив. Насправді пізнання навіть на рівні сприйняття - це активний процес збору інформації про зовнішній світ, який передбачає використання гіпотез, когнітивних карт, деякі з яких можуть бути вродженими. Потім в процесі мислення використовуються різноманітні знакові засоби. Пізнання може ставитися до тих предметів, яких ще немає (пізнання майбутнього), або яких вже немає (пізнання минулого). Догматизація «ленінської теорії відображення» ускладнювала дослідження низки проблем теорії пізнання, не дозволяла зіставляти це розуміння з іншими пізнавальними концепціями: феноменалізмом, інструменталізмом та ін.

Сучасна епістемологія науки трактує пізнання як філософську категорію, що описує процес побудови ідеал ^них 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. Відносно науки пізнання слід розуміти як процес, що супроводжує діяльність і спілкування людей і виконує функцію їх забезпечення ідеальним чином. Пізнання не стільки відображення, скільки має справу з 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 потреб;; ють 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, іцо 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 *внесення сенсу є реальність, створення ідеальних моделей, що дозволяють спрямовувати діяльність і спілкування і систематизувати акти свідомості.* Конструктивна перебудова пізнавальних структур дозволяє зд^лснювати перехід від одних стандартів людського досвіду до інших, надавати динамічність і творчий характер пізнавальному процесу.

Будь-яке *творче пізнання народжує віртуальні світи, створює передумови створення та існування культурних об'єктів взагалі. Сучасний інтерес до віртуалістики пов'язаний з методами розширення горизонту свідомості, створенАя передумов породження будь-якого об'єкта культури.*

Такі уявлення про пізнання в науці знаходять відгук у сучасного покоління дослідників і сприяють динамізму їх мислення, і *саме в цю концепцію треба вписувати сучасну криптографію.*

Тому головна критична претензія до автора дисертації: *її матеріал треба було включати в більш широкий філософський контекст і піддавати грунтовному методологічному аналізу.* Здається, що цей аспект має більш

значущий сенс, ніж обгрунтований дисертантом перехід до квантової криптографії.

Подарком дисертанту став великий матеріал з *історії криптографії.* Він не є набутим самостійно, але широко використаний, трансльований для цілей дисертації. Треба критично зауважити, що далеко не всі його методологічні ресурси ефективно використано. Висновки з цього матеріалу (а це два розділи дисертації) досить побіжні і тривіальні. Треба було головний акцент зробити на історії криптографії у XX столітті, на драматичних сторінках Першої и Другої світових воєн, змаганні держав в галузі шифрування інформації, виникненні перших машин, а головне - на наслідках інформатизації суспільства і науки. Цього фактично не було зроблено.

Недоліком роботи є також принцип наведення змісту використаних джерел: вони подаються списками, без виділення та аналізу тих з них, що є, на вибір дисертанта, найбільш значущими. Це також знижує рівень результатів дослідження.

Попри ці недоліки, фактом є дослідна допитливість і кваліфікація дисертанта, що дозволило йому виокремити і намітити шляхи вирішення великої проблеми сучасності - способів шифрування інформації з метою її захисту від незаконних користувачів. Дисертацію написано сучасною українською науковою мовою Матеріали дисертації достатнь) повно викладені у наукових публікаціях: 6 статях, одна з яких в закордонному журналі, 3 тезах науково-практичних конференцій. Всі вимоги ДАК МОИ України щодо наукових публікацій витримано. Зміст автореферату достатньо повно відображає зміст і результати дисертаційного дослідження.

Дисертація А.О. Михальчука відповідає вимогам, що висуваються до кандидатських дисертацій згідно «Порядку присудження наукових ступенів і вченого звання старшого наукового співробітника», затвердженого Постановою Кабінету Міністрів України від 24 липня 2013 р. № 567. Андрій Олександрович

Михальчук заслуговує присвоєння наукового ступеня кандидата філософських наук за спеціальністю 09.00.09 - філософія науки.

Офіційний опонент
кандидат філософських наук,
старший науковий співробітник
Державної установи «Інститут досліджень
науково-технічного потенціалу та історії науки
ім. Г.М. Доброва НАН України»

Онопрієнко М. В.

30.08.2019 р.

Підпис Онопрієнка М. В.
Засвідчую Тимофєєва О.О.
Зав. відділом кадрів

Національна академія наук України * Державна установа * м. Київ
"Інститут досліджень науково-технічного потенціалу та історії науки ім. Г.М. Доброва НАН України"
Ідентифікаційний код 13694464

Відгук надійшов до спец. вч. ради
16.09.2019 р.

УКРАЇНА * ІНСТИТУТ * КАНЦЕЛЯРІЯ