ВІДГУК

офіційного опонента

на дисертацію Михальчука Андрія Олександровича

«Феномен криптографії в контексті розвитку європейської науки»,

подану на здобуття наукового ступеня кандидата філософських наук

за спеціальністю 09.00.09 - філософія науки

Філософія та методологія науки як окрема філософська дисципліна розвинулася в XX ст. багато в чому як відповідь на потребу осмислення наукового пізнання, що перетворилося в цей час на одну з провідних і найбільш потужних сфер культури. Стрімкий розвиток новітніх технологій, який характеризує цивілізаційний поступ людства протягом кількох останніх десятиліть, не завжди супроводжується відповідним смислоутворенням, формуванням світоглядних орієнтирів буття людини в умовах складного техногенного світу, що виступає фактором, який здатний приводити до кризи - як особистісної, так і глобальної, на кшталт екологічної чи демографічної.

Бурхливе становлення інформаційних технологій, яке відбулося й відбувається буквально на наших очах, кардинально змінює звичне середовище людської життєдіяльності майже в усіх її сферах. Повсюдна комп'ютеризація та інтернетизація, з одного боку, спрощують життя, надаючи миттєвий доступ до велетенського обсягу інформації, проте з іншого - призводять до постановки нових проблем щодо орієнтування в цьому обсязі, засвоєння інформації, етичних аспектів її передачі та використання, - тобто, проблем, яким подекуди ще бракує належного осмислення. Вказані питання є тим більш актуальними у вітчизняних реаліях, що Україна, яка колись, за часів В. Глушкова, йшла в авангарді світового розвитку комп'ютерних технологій, на сьогодні втратила значну частину свого наукового потенціалу та передові позиції у цьому розвитку. Проте, новітні тенденції, зокрема стратегія формування електронного врядування та новітній проект «Україна у смартфоні» виступають для нашої країни історичним шансом, який водночас вимагає розв'язання цілої низки не

лише технологічних, а й соціальних, політичних, етичних і філософсько-методологічних проблем.

Саме тому слід підкреслити актуальність розробки питань інформаційної безпеки, пов'язаної з можливістю конфіденційної передачі будь-яких даних іншим особам, із забезпеченням інтегральної цілісності таких даних і збереженням авторства та відповідальності за зміст інформації, іцо передається, - і це тематика, яка відповідає колу компетенції такої сфери діяльності, як криптографія, та яка виступає досить новітньою для вітчизняної філософії науки. Втім, важко не погодитися з автором представленої до захисту дисертації на дану тему в тому, що проблематика розвитку криптографії та безпеки інформаційних даних становить значимий об'єкт для дослідження та філософського осмислення в галузі методології сучасної науки, якому поки що бракує уваги з боку дослідників.

Перш за все слід указати на значущість вже самої запропонованої А. О. Михальчуком постановки питання про криптографію як повноправний предмет дослідження в галузі філософії та методології наукового пізнання: взявши за мету розглянути статус та функції криптографії в контексті історичного розвитку науки, здобувач обґрунтовує динаміку зміни такого статусу від сукупності технологій кодування/декодування для захисту конфіденційних повідомлень до низки науково-технологічних методів, що використовувалися різними науками та паранауками, й аж до трансформації з технології та мистецтва шифрування на міждисциплінарну галузь наукового знання - криптологію. Отже, не зважаючи на новизну обраної дисертантом тематики, вона цілком відповідає паспорту спеціальності 09.00.09 - «філософія науки», оскільки охоплює собою історію та філософсько-методологічні засади криптографії та криптології як окремої наукової дисципліни.

За своєю структурою роботу здобувача побудовано логічно та послідовно. Перший розділ присвячено встановленню теоретико-методологічного підґрунтя дослідження: здійснено аналіз великої кількості джерел не лише з криптографії та філософії, а й із семіотики. Спираючись на розглянуті ідеї таких мислителів, як математик Джон Чедвік, Ч. Морріс,

Ч. Пірс, Ф. де Соссюр, У. Еко, Ю. Лотман, В. Глушков та in., автор приходить до обґрунтованого висновку про те, що феномен криптографії має розглядатися у трьох основних аспектах: з позицій філософсько-семіотичного підходу (як концепція коду і знака), у світлі підходу математично-лінгвістичного (як теорія і практика інтерпретації алгоритмів і систем захисту), та в річищі культурно-антропологічного підходу (як система культурних кодів, що має вплив на діяльність та інтелект людини) (с.38 дисертації). Значну уваги при цьому приділено формулюванню категоріально-понятійного апарату дослідження криптографії, яка визначається автором роботи як «сукупність технологій... кодування/декодування інформації будь-якими комунікаційними засобами, які забезпечують захищеність, цілісність, аутентичність й конфіденційність процесів передачі, обробки та зберігання даних» (с.41), і один із методів сучасної науки, здатний «формувати нову соціокультурну дійсність: науково-інформаційний вимір, у якому безпека даних є важливим компонентом наукової діяльності, що впливає на тенденції розвитку сучасного інформаційного суспільства» (с.59).

У другому розділі дисертації розглянуто динаміку розвитку криптографічної традиції в історії науки, починаючи від проблематики шифрів і кодування, якої торкався багато хто з давньогрецьких філософів. В результаті здійсненого автором аналізу Античність, Середньовіччя, Ренесанс і Новий час концептуалізовано як чотири етапи не просто історичного розвитку криптографії, а й зміни її змісту та статусу. За висновком автора, з появою спочатку аналітичних, а згодом і електронно-обчислювальних машин застосування криптографії розширюється і на соціогуманітаристику, і на науково-технологічну сфери, що сприяє зародженню теорії інформації з криптоаналізом в якості складової.

Найбільш змістовним і цікавим виявляється третій розділ дисертації, присвячений місцю та ролі криптографічних кодів у сучасному інформаційному науково-технічному просторі. Переконливо доводиться, що внаслідок трансформації наукової діяльності в річищі процесів інформатизації та комп'ютеризації змінюються й основні характеристики цієї діяльності

(с. 140), і в сучасній криптографії реалізується міждисциплінарний синтез фундаментальних і прикладних наук. Розглядаючи значення використання криптографічних кодів в Інтернет-комунікаціях та вплив систем захисту інформації на розвиток науки та людського інтелекту, автор демонструє добру обізнаність в галузі сучасної кібернетики та теорії інформації, аналізуючи праці К. Шеннона, Н. Вінера, А. Тьюрінга, В. Глушкова та інших науковців. Зроблені висновки є обґрунтованими та містять у собі елементи наукової новизни, вводячи криптографічну проблематику до кола сучасного дискурсу у галузі філософії та методології науки.

Разом із тим, не можна не зробити й деяких суттєвих зауважень до змісту та тексту поданої до захисту дисертаційної роботи.

По-перше, певні запитання викликає формулювання мети дисертації, деяких її завдань і підрозділів у сенсі обмеження предмета розгляду процесом розвитку саме європейської науки (с і 7 та ін.). Адже у своєму аналізі історичної динаміки становлення та розвитку криптографії автор звертається не лише до європейського досвіду, а й до праць Аль-КіндІ, що творив у Багдаді, або Евкліда з Александрії; як зазначається в роботі, «більшість із доступних нам найдавніших джерел» із цього предмету «сягають епохи Стародавнього Сходу» (с.64), - так само й суфізм (с.83) чи кабалістику (с.84-85) важко однозначно віднести до сфери суто європейської науки, - не кажучи вже про те, що за сучасної доби глобалізації спроби визначати будь-яку галузь наукового пізнання, а тим більше інформаційної науки, з точки зору *її* географічної приналежності виступають сумнівною справою..

По-друге, було би доречним приділити більше уваги дефініції, концептуалізації та розрізненню таких понять, як криптографія, криптоаналіз і криптологія. У темі роботи, у визначенні її мети фігурує поняття криптографія, яке постає, за висновком автора, в якості «поліфункціонального філософсько-наукового феномена», що становить собою складову криптології як науки (с.20), яка у свою чергу «складається з криптографії та криптоаналізу на основі синтезу фундаментальної й прикладної математики, фізики (квантової, лазерної, молекулярної, статистичної), лінгвістики, теорії інформації,

інформаційної безпеки тощо» (с193). Водночас, у тексті дисертації можна зустріти, з одного боку, такі твердження, як-от: «У своєму трактаті з криптології Аль Кінді зазначав, що одним із важливих способів дешифрування прихованого тексту є математичний обрахунок кожного знака» (с.26), а з іншого - вислови на кшталт: «Криптографія як наука базується на поєднанні методів філософії, математики, лінгвістики, культурології, риторики» (с.39), із чого можна зробити висновок, що в даному випадку терміни «криптологія» та «криптографія» використовуються автором чи не в якості синонімів, без чіткого розмежування криптографії як сукупності певних технологій - і криптології як наукової дисципліни. Категоріальний апарат як поданої дисертаційної роботи, так і філософії науки в цілому однозначно би збагатився, якщо б здобувач провів більш ретельну роботу з термінологічної обробки відповідних понять і дотримувався їх однозначного вживання у тексті.

По-третє, доводиться із жалем констатувати, що поза дослідницькою увагою дисертанта залишилося досить велике коло питань, пов'язаних із філософським осмисленням сучасних проблем інформаційної науки в цілому та криптографії зокрема, оскільки перевагу при розгляді цього феномена, який бурхливо розвивається саме в наші дні, була віддано історичній ретроспективі зміни його статусу, а не сучасним його особливостям. Можна згадати зокрема проблеми Інтернет-цензури та сітьової анонімності, що отримують цікаве осмислення в роботах представників такої течії думки, як криптоанархізм, представники якої прагнуть до забезпечення таємниці листування та інших свобод людини в умовах сьогоденних віртуальних спільнот і соціальних мереж.

Проте, вищенаведені зауваження не ставлять під сумнів новизну та практичну значимість дисертаційного дослідження А. О. Михальчука, але стосуються скоріше можливих напрямів подальшого опрацювання розпочатого в ньому філософського осмислення феномена криптографії. Дисертаційна робота відповідає профілю спеціалізованої вченої ради та паспорту обраної спеціальності - «філософія науки». Робота написана грамотною науковою мовою; її результати, відображені в положеннях наукової новизни, є значущими

для філософського осмислення сучасної науки та обґрунтованими в тексті дисертації.

Результати дослідження пройшли належну наукову апробацію, про що свідчить наявність восьми наукових праць здобувача, чотири з яких опубліковані у фахових виданнях України, одна стаття – у періодичному закордонному виданні, що входить до міжнародних наукометричних баз, та три тези доповідей на міжнародних науково-практичних конференціях. Автореферат рецензованої дисертації відповідає вимогам МОН України до оформлення авторефератів кандидатських дисертацій, його зміст ідентичний основним положенням дисертаційної роботи та дає повне й адекватне уявлення про загальну характеристику та структуру роботи, послідовність виконання дослідницьких завдань, отримані здобувачем висновки.

Актуальність і рівень розкриття поставлених проблем, новизна теми дисертації та ступінь обґрунтованості винесених на захист наукових положень відповідають вимогам МОН України до кандидатських дисертацій та п. 11, 13 «Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника», затвердженого Постановою Кабінету Міністрів України № 567 від 24 липня 2013 року. У відповідності до зазначеного можна зробити висновок, що дисертація А. О. Михальчука «Феномен криптографії в контексті розвитку європейської науки» відповідає нормативним вимогам МОН України, а її автор заслуговує на присудження йому наукового ступеня кандидата філософських наук зі спеціальності 09.00.09 – філософія науки.

Офіційний опонент
доктор філософських наук,
провідний науковий співробітник
відділу інтернаціоналізації вищої освіти
Інституту вищої освіти НАПН України *Мєлков Ю. О.*

Підпис Мєлкова Ю.О. засвідчую.
Заступник завідувача відділу науково-організаційної та кадрової роботи Інституту вищої освіти НАПН України.
/Степанова Г.В.
10.09.2019 р.