УДК 004.312.26

ЛІСОВСЬКА Ю.П., *кандидат юридичних наук.*
ORCID: https://0000-0001-9278-4487.

СУЧАСНІ ПЕРСПЕКТИВИ РОЗВИТКУ КВАНТОВОЇ БЕЗПЕКИ ЯК ДИФУЗІЙНО ЯКІСНА ЦИФРОВА МОДЕЛЬ У МІЖНАРОДНІЙ ІНФОРМАЦІЇ ЗНАНЬ

Анотація. *Стаття досліджує розвиток криптографічних засобів захисту інформації, міжнародні і нові вітчизняні стандарти криптографічного захисту, які дозволяють користувачам відчувати впевненість у захисті конфіденційної інформації. Виділено ряд загроз, які, згідно з прогнозами аналітиків, набудуть актуальності в найближчому майбутньому. У роботі було проведено аналіз використання квантових технологій у сфері кібербезпеки. Виявлено, що зі створенням квантового комп'ютера квантова криптографія стане одним з найнадійніших способів захисту інформації. Висвітлено загрози з боку квантового комп'ютинга, сучасної науки, яка стрімко розвивається.*

Ключові слова: *криптографія, захист, загрози, квантова безпека, контррозвідувальна діяльність.*

Summary. *The article considers the development of cryptographic means of information security, international and new domestic standards of cryptographic protection, which allow users to feel confident in the protection of confidential information. A number of threats have been identified that, according to analysts, will become relevant in the near future. In this paper, we analyzed the use of quantum technologies in the field of cybersecurity. It has been revealed that with the creation of a quantum computer, quantum cryptography will become one of the most reliable ways to protect information. Their coverage – the threats from quantum computing, modern science, which is developing rapidly.*

Keywords: *cryptography, protection, threats, quantum security, counterintelligence activity.*

Аннотация. *Статья исследует развитие криптографических средств защиты информации, международные и новые отечественные стандарты криптографической защиты, которые разрешат пользователям чувствовать уверенность в защите конфиденциальной информации. Выделены ряд угроз, которые, согласно прогнозам аналитиков, приобретут актуальность в ближайшем будущем. Проведен анализ использования квантовых технологий в области кибербезопасности. Выявлено, что с созданием квантового компьютера квантовая криптография станет одним из самых надежных способов защиты информации. Освещены угрозы со стороны квантового компъютинга, современной науки, которая стремительно развивается.*

Ключевые слова: *криптография, защита, угрозы, квантовая безопасность, контрразведывательная деятельность.*

Постановка проблеми. Сучасна система кодифікованого пізнання знань пропонує до вибору кожної особи на рівні держави та суспільства надзвичайно розмаїтий спектр галузей наук, спеціальностей та спеціалізацій. За цих умов актуального значення набуває антикорупційна освіта, що дозволяє виробити на практиці законодавчі механізми її інноваційного забезпечення та реалізацію мудрих рішень до суперечливих умов життя. Така Людина XXI століття – це Людина універсального мислення, котра здатна відстежувати міждисциплінарні та міжкультурні смислоутворюючі горизонти складної глобалізованої дійсності, не замикаючись в межах своєї вузької фахової орієнтації.

Світоглядні основи формування та розвитку творчої особи знайшло відображення у сучасному кіберпросторі, де квантова безпека як одна із нових електронно-цифрових сфер наукових категорій ґрунтується на екзистенційному вимірі освітнього самоздійснення у конструктологічну єдність. При цьому, квантова безпека як корпускулярно-хвильова структура сфокусованого випромінювання у вигляді потужно енергетичних "порцій" космічного світла і віднаходить приклад доцільності інтерпретації людського персонального та професійного життя на тлі екзистенційних настанов мудрості в сучасних умовах міжнародної інформації знань.

Результати аналізу наукових публікацій. Проблематика сучасного безпекознавства, в якому структурна модель квантової безпеки займає важливе місце у міждисциплінарних дослідженнях, є невичерпною у міжнародній інформації знань. До таких питань лише торкаються такі вітчизняні вчені як Баранов О.А., Ільченко М.Ю., Курко М.Н., Ліпкан В.А., Марущак А.І., Макаренко Є.А., Остроухов В.В., Рябека О.Г., так і зарубіжні – Фукуяма Ф., Хакен Г., Урсул А., Сулер Д., Маритен Ж. тощо.

Метою статті є оцінка проблем та їх вирішення у сучасної квантовій безпеці на основі дифузійно якісного цифрового переосмислення системи міжнародної інформації знань в життєвих реаліях.

Виклад основного матеріалу. У сучасних умовах інформаційного розвитку країн світу виникли питання становлення та забезпечення доступу людини та громадянина до інформації, яка перебуває у володінні не лише органів державної влади, а й олігархату як кланової моделі в корумпованому середовищі.

Квантова безпека як програмний криптоалгоритм щодо кіберзахисту прав та свобод громадянина на інформацію.

Екзистенційні виміри людини на підставі внутрішніх переживань та страждань як вияву емоційно-чуттєвої сфери її свідомості дозволяють виходити за межі наявного буття в трансцендентні виміри людинокосмізму. Адже "буття постає як конкретна відкритість до своїх безмежних можливостей та здатність проблематизації власних підстав. У стосунку до нього людина уникає загубленості в розрізнених життєвих ситуаціях та протистоїть уніфікуючій потребі продукувати і здобувати" [1, с. 332-345].

При цьому потрібно відзначити, що саме квантова безпека як програмний криптоалгоритм комп'ютерних систем і створює інституціональний підхід щодо гуманної свободи інформації в міжнародному демократичному просторі. Зокрема, загальні концептуальні положення були сформульовані в рамках Організації Об'єднаних Націй та інших міжнародних організацій і полягають у визначенні загальноприйнятих моделей щодо свободи інформації, основних принципів, законодавчих основ, ролі інституту міжнародно інформаційних відносин та значення його в системі демократичного розвитку сучасного суспільства [1, с. 450-452].

За цих обставин квантова безпека сприяє комп'ютерному обчисленню із застосуванням якісної технології CUDA, оскільки багатофункціональні паралельні мови, такі як CUDA і Opencl, зменшили складність програмування. Однак, щоб повною мірою скористатися їх обчислювальною потужністю, потрібно самоздійснювати програмування завдяки відповідному криптоалгоритму. Крім того, ієрархія пам'яті графічного процесора і багатопотокова архітектура є складним програмуванням для досвідчених програмістів [2, с. 232].

Правовий механізм контррозвідувального контролю у системі квантової безпеки.

Сучасна контррозвідка, що захищає правові інтереси особи, держави та суспільства в умовах нових інформаційних технологій, повинна цілісно оперувати інтерференційними та резонансними підходами у системі квантової безпеки. Адже

контррозвідувальна діяльність потребує від співробітника спецслужб опанування загальних знань як природного вжитку, так і набутих в результаті освітнього самоздійснення. Для цього в постфактах незалежно та професійно *контррозвіднику* необхідно діяти проактивно за обставинами, при цьому бути надто спостережливим, гнучким (дипломатичним), сприяти координації та контролю правоохоронних органів та військовим формуванням, а також згідно чинного законодавства ефективно надавати криптоаналітичну оцінку в системі превентивних заходів квантової безпеки. Все це вимагає мобільного проведення широкомасштабних контррозвідувальних робіт щодо електромагнітних властивостей метеополя та параметрів сучасної геодинаміки "у залежності від ступеню гетерогенності середовища й просторово-часового масштабу об'єктів і явищ та переходу до довгоперіодичних рядів аерокосмічних спостережень (моніторингу) з лазерним використанням високоточного приладного парку в рамках міжнародно-правових проектів і національних програм" [4, с. 86].

У свою чергу, коли сучасна інформаційна сфера суспільства семантично ініціює якісно нову перехідну модель квантової безпеки, критеріально використовуються інноваційні процеси спецслужб держав світу за умов ентропії, балістики та логістики. Формування в такий спосіб інформаційного капіталу мудрості держави та громадськості як ментально-смислових цінностей істини надає поштовх для консолідації окремої (кожної, всіх) нації та щодо пошуків збалансованого взаєморозуміння у міжвідомчому партнерстві світу. "Важливого балансу …можливо досягти шляхом ретельного аналізу із якомога ширшим залученням до процесу прийняття рішень як урядовців, так і громадян. Такий підхід забезпечуватиме демократичні принципи вибору, які ґрунтуватимуться на гуманній поінформованості щодо можливих альтернатив" [3, с. 67-78].

Інформаційна логістика в квантовій безпеці.

Інформаційна логістика – це напрям логістики, що оперативно координує та контролює потоки інформації, яка зберігається, обробляється та розподіляється за рахунок квантової (електронно-перехідної дифузії) взаємодії між собою. Іншими словами, "логістика – це наука про організацію, планування, контроль і регулювання руху матеріальних, а також інформаційних потоків у просторі і в часі від їх первинного до кінцевого споживача" [5, с. 158].

Основним критерієм інформаційної логістики є системна самоорганізація її квантово (в даному разі інтенційно, точково) обумовлених режимних потоків енергії. Завдяки такому мультивібраційному процесу усі елементи інформаційної системи безвинятково повинні працювати злагоджено як одне ціле. Наявним прикладом сьогодні може слугувати правова діяльність Офісу генерального прокурора, в якій прокурор відділу розгляду звернень громадян управління організації прийому громадян, розгляду звернень та запитів оперативно, в квантовому режимі, здійснює за належністю заявника (ініціатора скарги) організацію перевірки та прийняття рішення відповідно до вимог чинного законодавства. Важливим елементом таких інформаційних технологій, як всім відомо, є використання штрих-коду, що унеможливлює спотворення інформації, викрадення. В цілому, така інформаційна логістика забезпечує аналіз і консолідацію очевидних контактів та лідерський діалог зі світовими партнерами як неолобістський рух у майбутнє, закріплений міжнародно-правовими нормами та стандартами.

Крім того, акцентуючи увагу на складній системі квантової безпеки, до необхідної інформації повинні бути допущені лише ті особи, які безпосередньо мають право на виконання певних операцій. У цьому змісті, від несанкціонованого проникнення в інформаційну логістику повинна захищати структурна організація квантової безпеки даних, що надає можливість гнучкого налаштування і регулювання відповідних

параметрів. Отже, з огляду на це, розробка в інформаційній логістиці саме сучасної *квантової комп'ютеризації* як системи програмного і математичного забезпечення оптимізує та організує нове суспільство знань як перехід від моральної деградації в певному молодіжному середовищі до потужно-енергетичного ресурсу (феноменальної пам'яті) в інтелектуальному середовищі.

Кібернетичний захист квантової безпеки щодо норми правової поведінки особи в антикорупційній освіті.

Специфіка кібернетичного захисту квантової безпеки орієнтує міжнародно-правове дослідження "на розкриття цілісності об'єкта та механізмів, які її забезпечують на виявлення різноманітних типів зв'язків складного об'єкта і інформаційного зведення їх в єдину теоретичну картину" [6, с. 96]. До того ж, у морально-розрихле середовище "хлинула хвиля нечесті, відходів Західної, та й Східної, цивілізації. Ситуація не просто загострилася, вона стала нестерпною… Широке поширення в молодіжному середовищі одержали такі несумісні з мораллю речі, як наркоманія й алкоголізм, злодійство і рекет, знущання над особистістю і звичайна підлість. Здається, що підлих людей, які забули про жаль, милосердя й елементарну совість, стало більше. Моральна деградація суспільства стає небезпечною" [7, с. 432].

З боку антикорупційної освіти необхідно використовувати всілякі канали впливу, пояснювати кожному державному діячу, що освіта в системі міжнародної інформації знань – це той інтелектуальний ресурс, який здобувається особистістю шляхом належної суспільної і державної організації і забезпечення. Принциповим стало положення про забезпечення усім і кожному рівного доступу до якісної освіти; утвердження новітніх інформаційних технологій; впровадження мовних стратегій освіти; демократизація освіти і її адаптація до ринкових перетворень: підвищення конкурентоздатності у світовому освітньому просторі.

Як відомо, Болонський процес (назва походить від університету Болонья, Італія, де були досягнуті відповідні домовленості) – це своєрідний рух освітніх національних систем до єдиних критеріїв і стандартів, які утверджуються в європейському просторі. "Його мета полягає в консолідації зусиль наукової та освітянської громадськості й урядів країн Європи для істотного підвищення конкурентоздатності європейської вищої освіти і науки у світовому вимірі, а також для підвищення ролі цієї системи" [7, с. 431]. Цей рух обумовлений реальними змінами, що відбуваються на теренах Європи і світу, а також є своєрідною відповіддю на виклики глобалізації, становлення інформаційного суспільства знань у відповідності зі спільними правовими нормами і стандартами.

Практичні заходи квантової безпеки у протидії корумпованій злочинності в сучасній Україні.

З метою створення на базі сучасних цифрових технологій єдиної багаторівневої міжвідомчої спеціальної інформаційно-телекомунікаційної системи з елементами централізованого управління для забезпечення захищеного інформаційного обміну проводяться роботи із створення Національної телекомунікаційної мережі, зокрема:

- підготовлено техніко-економічне обґрунтування "Будівництво Національної телекомунікаційної мережі" та проведено державну будівельну експертизу, за результатами якої отримано від державного підприємства "Укрдержекспертиза" позитивний висновок (техніко-економічне обґрунтування схвалено наказом Адміністрації Держспецзв'язку від 11 жовтня 2017 р. № 557);

- підготовлено, проведено державну будівельну експертизу та затверджено проектну документацію (стадія "П") Національної телекомунікаційної мережі (перша черга) (наказ Адміністрації Держспецзв'язку від 7 грудня 2017 р. № 668);

- укладено договір підряду на будівництво першої черги Національної телекомунікаційної мережі між Головним управлінням урядового зв'язку Держспецзв'язку та ПрАТ "Пріоком";

- завершено виконання монтажних робіт з розгортання та підключення 21 транспортного вузла Національної телекомунікаційної мережі в облдержадміністраціях України, а також проведено пусконалагоджувальні роботи на зазначених вузлах та введено їх в експлуатацію;

- підготовлено та затверджено проектну документацію ескізного проекту "Створення Центру обробки даних Національної телекомунікаційної мережі".

Також для забезпечення кіберзахисту:

- модернізовано існуючу Систему захищеного доступу державних органів до Інтернету, яка довела свою ефективність під час протидії кібератакам, що здійснювалися протягом 2017 року. Жоден державний електронний ресурс, який був захищений зазначеною Системою, не постраждав. Ця Система на сьогодні забезпечує захист інформації веб-ресурсів Адміністрації Президента України, Національного антикорупційного бюро, Служби зовнішньої розвідки, СБУ, МЗС, ДФС, Центральної виборчої комісії та Луганської облдержадміністрації. Проведена модернізація дасть змогу підключити до Системи більшу кількість абонентів;

- забезпечено функціонування Команди реагування на комп'ютерні надзвичайні події України (CERT-UA), яка у взаємодії з правоохоронними органами та міжнародними командами реагування на кіберінциденти здійснила відповідні заходи щодо реагування та мінімізації наслідків кібератак (ШПЗ WannaCry, Petya.A). Протягом 2017 року вищезазначеною Командою забезпечено реагування на понад 200 комп'ютерних інцидентів, що могли призвести до порушення сталого режиму функціонування державних інформаційно-телекомунікаційних систем (поінформовано правоохоронні органи).

Разом з тим введено в дію (2 лютого 2018 р.) Центр реагування на кіберзагрози Держспецзв'язку. Центр реагування на кіберзагрози (*Cyber Threat Response Centre, CRC*) побудовано на базі найновітніших досягнень у сфері кіберзахисту як вітчизняних, так і провідних ІТ-компаній світу. Розроблені на рівні кращих світових аналогів сучасні технологічна та аналітична системи CRC закономірно претендують на звання найпотужніших в європейському співтоваристві. Завдяки втіленим у Центрі реагування на кіберзагрози унікальним технологічним рішенням Держспецзв'язку здатна з високим ступенем точності здійснювати у режимі "24/7" раннє виявлення аномальних активностей та потенційно небезпечних подій у системах і мережах, підключених до Інтернету. Час реагування на кіберзагрози та сповіщення про них скоротився в десятки разів.

Таким чином, Центр реагування на кіберзагрози – це технічна платформа взаємодії основних суб'єктів забезпечення кібербезпеки (Держспецзв'язку, СБУ, Національної поліції), що підвищує рівень ефективності і оперативності діяльності правоохоронних структур з протидії та розслідування кіберзлочинів, ефективний механізм координації зусиль усіх учасників кіберзахисту державного і приватного секторів, який є однією з ключових ланок прийняття оперативних рішень Національним центром кібербезпеки Ради національної безпеки і оборони України.

Висновки.

Кібербезпека як фактор міжнародних відносин, вплив якого має універсальний характер і враховується як в діяльності міжнародного співтовариства, так і в зовнішній політиці окремих держав, призводить до трансформації самої сутності проблеми безпеки після закінчення "холодної війни" і розпаду біполярної міжнародної системи, до

поведінки міжнародних акторів, викликаючи концептуальний перегляд принципів функціонування міжнародних і національних інститутів, що відповідають за глобальну безпеку, а також обліку в нових доктринах міжнародної безпеки інформаційної складової. Конфліктогенність глобальних інформаційних процесів викликає поява нових диспропорцій в міжнародній системі: на основі інформаційних факторів з'явилася проблема інформаційного дисбалансу між розвиненими країнами і країнами, що розвиваються.

Використана література

1. Хайдеггер М. Бытие в окрестности вещей. Москва: Фолио, 1998. 509 с.
2. Боресков А.В., Харламов А.А. Основы работы с технологией CUDA. Москва: ДМК Пресс, 2010. 232 с.
3. Давыденко В.В. Социальный диалог: проблема достижения стандартов Евросоюза. *Политический менеджмент*. № 2/2006. С. 67-78.
4. Макаренко Є.А. Міжнародна інформаційна політика: структура, тенденції, перспективи [дисертація]. Київ: Національ. ун-т ім. Т. Шевченка, 2003. 475с.
5. Губенко В.К. Логистическая цнтрализация материальных потоков: теория и методология логистических распределительных центров. Донецк: Институт экономики и промышленности, 2007. 495 с.
6. Баскаков А.Я**.** Методология научного исследования. Киев: МАУП, 2004. 216 с.
7. Андрущенко В. Організоване суспільство: проблеми суспільної саморганізації та інституціоналізації в період радикальних трансформацій в Україні на рубежі століть. – (Досвід соціально-філософського аналізу). Київ: Знання України, 2018. 630 с.
8. Курко М.Н., Лісовський П.М., Лісовська Ю.П. Криптологія. Київ: Видавничий дім "Кондор", 2020. 248 с.
9. Лісовський П.М, Лісовська Ю.П. Національна безпека України: навч. посіб. Київ: Університет "Україна", 2020. 292 с.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~