ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації Абрамова Сергія Вадимовича на тему «Моделі та методи підвищення швидкодії алгоритму CSIDH на основі суперсингулярних кривих Едвардса», поданої на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека

Актуальність теми дослідження.

Дисертаційна робота присвячена вирішенню актуального наукового завдання, сутність якого полягає в підвищенні захищеності і швидкодії у постквантових умовах криптосистем на основі CSIDH (англ. Commutative Supersingular Isogeny Diffie–Hellman,) комутативної криптосистеми Діффі-Геллмана на основі ізогеній суперсингулярних кривих. Ця система є одною з лідерів асиметричних постквантових криптосистем, яка збудована на ізогеніях і тому резистивна до атак квантових комп'ютерів, які, як очікується, з'являться у найближчому майбутньому. Але крім квантової резистентності ця система має недостатню швидкість та захищеність від атак стороннього каналу. Тому збільшити, у першу чергу, ці характеристики є актуальним і важливим завданням.

Для реалізації завдання пропонується будувати системи CSIDH на ґрунті ізогеній нециклічних суперсингулярних кривих Едвардса як пар квадратичного кручення. Використання еліптичних кривих Едвардса значно підвищує захищеність криптоалгоритму, але при цьому збільшується складність обчислення алгоритму і відповідно зменшується його швидкодія. Тому є актуальною проблема підвищення швидкодії за рахунок модифікації цього алгоритму.

Таким чином, криптоалгоритм Діффі-Геллмана на ізогеніях еліптичних кривих є одним з найбільш перспективних для використання у постквантовий період. Дослідження щодо вдосконалення і модифікації криптоалгоритму Діффі-Геллмана на ізогеніях еліптичних кривих є актуальним завданням.

Для модифікації криптоалгоритму Діффі-Геллмана було обрано еліптичні криві у загальній формі Едвардса, які мають найкращі властивості серед інших кривих: найкоротший ключ і найбільшу швидкість. Запропоновано використовувати нециклічні криві з рандомізованим вибором, спростити метод обчислення ізогеній, рандомізувати і оптимізувати вибір ізогеній, спростити метод обміну ключами за рахунок інкапсуляції ключа, використовувати паралельні обчислення.

Дослідження щодо вдосконалення алгоритму CSIDH на основі скручених суперсингулярних кривих Едвардса є актуальним через його узгодження з поточними та майбутніми викликами кібербезпеки, вирішення проблем, пов'язаних із передаванням персональних, конфіденційних та секретних динних, а також еволюцією методів криптоаналізу. Воно забезпечує адаптивні підходи до безпеки, необхідної для забезпечення крипостійкості протоколів,

які функціонують у локальних та глобальних інформаційно-комунікаційних системах.

Особистий внесок здобувача полягає у виборі теми дисертації, обґрунтуванні та формулюванні мети, об'єкта, методів досліджень, визначенні завдань наукового дослідження, проведенні теоретичного обґрунтування та обробленні й аналізі даних, формулюванні висновків. В дослідженні автором:

- проаналізовано поточний стан і властивості класичних криптоалгоритмів Діффі-Геллмана, які працюють на еліптичних кривих і мають відмінні криптографічні параметри;

– визначено можливості покращення роботи криптоалгоритмів Діффі-Геллмана на ізогеніях еліптичних кривих, які здатні працювати у постквантових умовах при здійсненні атак з боку потужних квантових комп'ютерів;

– визначено властивості кривих Едвардса як оптимальних кандидатів для використання у постквантових алгоритмах;

– обґрунтовано клас і досліджено властивості еліптичних кривих Едвардса, які мають найкращі характеристики для використання у постквантових алгоритмах;

– визначено властивості алгоритму CSIDH на кривих Едвардса і обґрунтовано застосування алгоритмів CSIDH на нециклічних кривих;

– пришвидшено обчислення ізогенії для збільшення швидкодії криптоалгоритму та захисту від атаки сторонніми каналами;

– розроблено модифікації алгоритму CSIDH і створено комбінований криптоалгоритм із застосуванням його модифікацій;

– оцінено величину парціального зростання швидкості від кожної модифікації криптоалгоритму CSIDH на ізогеніях суперсингулярних еліптичних кривих Едвардса;

– розроблено модель алгоритму з використанням несуперсингулярних кривих Едвардса (НКЕ) і оцінено приріст швидкодії і криптографічної стійкості паралельних обчислень;

– оцінено інтегральний виграш у швидкодії модернізованих алгоритмів CSIDH і комутативної інкапсуляції ключа суперсингулярної ізогенії (від. англ. Commutative Supersingular Isogeny Key Encapsulation, CSIKE).

Зв'язок роботи з науковими програмами, планами, темами. Напрям дисертаційного дослідження безпосередньо пов'язаний з реалізацією доктрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії кібербезпеки України. Дисертаційна робота виконана відповідно до планів наукової і науково-технічної діяльності Київського столичного університету імені Бориса Грінченка в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (№0122U200483, КСУБГ, м. Київ). Також результати наукових досліджень прийняті до впровадження в діяльність Київського столичного університету імені Бориса Грінченка (акт

від 12.09.2024 року) та Інституту програмних систем Національної академії наук України (акт від 02.09.2024 року).

Мета дослідження полягає в підвищенні швидкодії і безпеки постквантового асиметричного криптоалгоритму CSIDH шляхом його моделювання і модернізації з використанням властивостей еліптичних кривих у формі Едвардса.

Завдання дослідження:

– проаналізувати поточний стан і властивості класичних криптоалгоритмів Діффі-Геллмана, які працюють на еліптичних кривих і мають відмінні криптографічні параметри;

– визначити можливості покращення роботи криптоалгоритмів Діффі-Геллмана на ізогеніях еліптичних кривих, які здатні працювати у постквантових умовах при здійсненні атак з боку потужних квантових комп'ютерів;

– визначити властивості кривих Едвардса як оптимальних кандидатів для використання у постквантових алгоритмах;

– обґрунтувати клас і досліджено властивості еліптичних кривих Едвардса, які мають найкращі характеристики для використання у постквантових алгоритмах;

– визначити властивості алгоритму CSIDH на кривих Едвардса і обґрунтовано застосування алгоритмів CSIDH на нециклічних кривих;

– пришвидшити обчислення ізогенії для збільшення швидкодії криптоалгоритму та захисту від атаки сторонніми каналами;

– розробити модифікації алгоритму CSIDH і створено комбінований криптоалгоритм із застосуванням його модифікацій;

– оцінити величину парціального зростання швидкості від кожної модифікації криптоалгоритму CSIDH на ізогеніях суперсінгулярних еліптичних кривих Едвардса;

– розробити модель алгоритму з використанням несуперсингулярних кривих Едвардса (НКЕ) і оцінено приріст швидкодії і криптографічної стійкості паралельних обчислень;

– оцінити інтегральний виграш у швидкодії модернізованих алгоритмів CSIDH і комутативної інкапсуляції ключа суперсингулярної ізогенії (від. англ. Commutative Supersingular Isogeny Key Encapsulation, CSIKE).

Об'єкт дослідження: процес перетворення інформації за допомогою асиметричної криптосистеми, що базується на складності пошуку графа ізогенного ланцюга між еліптичними кривими у формі Едвардса.

Предмет дослідження: моделі і методи підвищення швидкодії на основі скручених суперсингулярних кривих Едвардса (СКЕ) над простими полями F_p для створення паралельних криптосистем.

Методи дослідження. Для проведення досліджень в дисертаційній роботі використовувалися методи теорії чисел; теорії поля; теорія графів; теорія функцій; теорія алгоритмів; теорія односторонніх функцій; теорія складності алгоритмів; теорії ймовірностей та математичної статистики; абстрактної алгебри; алгебраїчної геометрії; математичне і комп'ютерне моделювання.

Експериментальна база дослідження. Достовірність дисертації підтверджується повторюваністю результатів реалізації моделей, документами про впровадження у діяльність кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка (акт № 18/1 від 12.09.2024 року), Інститут програмних систем Національної академії наук України (Київ, акт від 02.09.2024 року), а також опублікованими працями та апробацією результатів наукового дослідження на конференціях.

Наукова новизна одержаних результатів полягає в подальшому розвитку і обґрунтуванні методів підвищення ефективності постквантових криптоалгоритмів на ізогеніях еліптичних кривих Едвардса:

1. Вперше запропоновано і обґрунтовано метод підвищення швидкодії криптосистеми CSIDH шляхом використання замість одної циклічної повної кривої Едвардса двох нециклічних кривих з випадковим вибором однієї з кривих пари. Це у зрівнянні з CSIDH вдвічі розширює простір еліптичних кривих, спрощує обчислення параметра d кривих. Оцінка виграшу в швидкодії складає 2^5 рази. Використання додатково ізоморфних кривих породжує існування двох незалежних криптосистем з можливістю паралельних обчислень. Це додатково усуває загрозу атаки сторонніми каналами, подвоює швидкодію або довжину секретного ключа у два рази.

2. Вперше запропоновано модель інкапсуляції ключа CSIKE з рандомізацією з одним сеансом передачі і одним відкритим ключем замість двох у порівнянні з CSIDH. Модель ґрунтується на випадковому виборі однієї з нециклічних кривих Едвардса та випадковому виборі ступеня ізогенії на кожному кроці ланцюжка ізогеній. Такий випадковий вибір є альтернативою методам вирівнювання часу виконання групової операції постійного часу CSIDH, що не викликає штучного збільшення часу виконання алгоритму і усуває загрозу атаки сторонніми каналами. Це дозволяє удвічі скоротити час на обмін ключами і підвищує загальну швидкодію у два рази.

3. Удосконалено метод обчислення і вибору структури ізогеній у криптоалгоритмах CSIDH на кривих Едвардса. Обчислення ізогенних функцій функції $\varphi(R)$ випадкової точки R замінюється на більш просте обчислення параметру d ізогенної кривої. При цьому виконуються менш затратні операції, пов'язані зі скалярними множеннями випадкових точок на число, що прискорює обчислення порядку точок і надає прискорення алгоритму більш ніж у 2^3 разів. Вибір структури ступенів ізогеній за рахунок скорочення їх діапазону дає лінійну оцінку прискорення алгоритму в 1,5 рази.

4. Набув подальшого розвитку метод CRS на несуперсингулярних (ординарних) кривих та поділу секретів Діффі-Геллмана на ізогеніях ординарних нециклічних кривих Едвардса. Замість двох ізоморфних криптосистем в алгоритмі CSIDH перехід до НКЕ породжує чотири незалежні криптосистеми з можливістю паралельних обчислень. Це дає оцінку виграшу швидкості обчислень у чотири рази. Оцінка загального виграшу швидкості обчислень досягає $3 \cdot 2^9$ разів.

Теоретичне значення результатів дисертації. Результати досліджень представлені у вигляді наукових положень, висновків і рекомендацій. Розроблені автором і викладені у дисертації наукові положення, висновки та пропозиції мають високий рівень обґрунтованості. Опрацьовано значну кількість наукових та фахових джерел вітчизняних і зарубіжних вчених, здійснено їх аналіз та запропоновано власні підходи, що стосуються підвищення швидкодії криптопротоколів, що обробляється в інформаційно-комунікаційних системах підприємств критичної інфраструктури та державних органів.

Дисертація характеризується науковою глибиною та логічністю. Абрамов С.В. володіє ґрунтовними знаннями предмета дослідження, а також методології досліджень. Основні положення, висновки та рекомендації теоретичного та практичного характеру є обґрунтованими та достовірними. Результатом проведеного наукового дослідження є досягнення визначеної мети шляхом виконання поставлених дисертантом завдань, про що свідчать висновки до кожного розділу та дисертації загалом.

Практичне значення результатів дисертації полягає в наступному: динамічний розвиток технологій дешифрування призводить до появи потенційних можливостей злому існуючих алгоритмів шифрування за допомогою методів PQC, що, в той самий час, призводить до появи нових потенційних загроз для підприємств критичної інфраструктури, державних органів, приватного сектору та окремих громадян.

Саме ці тренди обумовлюють практичну значущість запропонованих в дослідженні методів вдосконалення систем шифрування на основі еліптичних кривих Едвардса. Розвинуто для практичного використання ланцюжків ізогеній еліптичних кривих Едвардса над простими полями в PQC криптоалгоритмах схеми Діффі-Геллмана для підвищення швидкодії та безпеки в умовах атак сторонніми каналами. Розроблено нові науково обґрунтовані методи і алгоритми функціонування криптосистеми на основі арифметики ланцюжків ізогеній еліптичних кривих Едвардса, що зменшує складність розрахунків до $3 \cdot 2^9$ разів у порівнянні з алгоритмами, які використовуються у попередніх алгоритмах. Запропоновано новий метод і створено відповідну комп'ютерну програму розрахунку ізогеній, у якої обчислюється тільки один параметр d кривої Едвардса без складного розрахунку ізогенної функції $\varphi(R)$, що значно підвищує швидкість роботи алгоритму. А з урахуванням сучасних вимог щодо стійкості і швидкості асиметричних криптосистем пропонується застосування суперсінгулярних квадратичних і скручених еліптичних кривих Едвардса для використання в сучасних асиметричних криптосистемах. Також отримано моделі алгоритмів на ізогеніях нециклічних СКЕ, які можна використовувати на практиці з врахуванням пропонованих модернізацій. Для практичного застосування потриманих наукових результатів розроблено програмне забезпечення, яке дозволяє виконати моделювання та тестування запропонованих криптосистем.

Апробація результатів дисертації. Основні теоретичні та практичні результати були представлені та обговорені в ході ряду наукових конференцій:

1. Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), 2022, 2023 (двічі) і 2024 (м. Київ).

2. Workshop on Classic, Quantum, and Post-Quantum Cryptography (CQPC), 2023 (м. Київ).

3. Цифрова трансформація фінансової системи України та країн V-4 в умовах євроінтеграції, 2024 (м. Дубляни).

4. Інформаційно-комунікаційні технології та кібербезпека (ІКТК), 2024 (м. Харків).

Публікації. Основні результати дисертації висвітлено у 11 наукових публікаціях, із них усі у співавторстві: 1 стаття (у співавторстві) у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України; 3 статті (з них усі у співавторстві) у періодичних наукових виданнях, проіндексованих в наукометричних базах даних Scopus і Web of Science Core Collection; 7 наукових публікацій (з них 5 у співавторстві), у яких додатково відображено результати дисертації. Наукові результати дисертації повною мірою висвітлено у наукових публікаціях.

Наукові статті, опубліковані у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України:

1. Bessalov, A., Kovalchuk, L., & Abramov, S. (2022). Рандомізація алгоритму CSIDH на квадратичних та скручених кривих Едварда. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 1(17), 128–144. https://doi.org/10.28925/2663-4023.2022.17.128144

Наукові статті, опубліковані у періодичних наукових виданнях, проіндексованих у базах даних Scopus і Web of Science Core Collection:

1. Bessalov, A., & Abramov, S. (2022). Special Properties of the Point Addition Law for Non-Cyclic Edwards Curves. *Cybernetics and Systems Analysis*, 58(683), 851–861. 2022 https://doi.org/10.1007/s10559-023-00518-w (Scopus Q3)

2. Bessalov, V., & Abramov, S. (2023). PQC CSIKE Algorithm on Non-Cyclic Edwards Curves. *Cybernetics and Systems Analysis*, 59(6), 867–879. 2023 https://doi.org/10.1007/s10559-023-00622-x (Scopus Q3)

3. Bessalov, A., Sokolov, V., & Abramov, S. (2024). Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves. *Cryptography*, 8(3), 1–17. https://doi.org/10.3390/cryptography8030038 (Scopus Q2 & WoS)

Наукові публікації, у яких додатково висвітлено результати дисертації:

1. Bessalov, A., Sokolov, V., Skladannyi, P., Abramov, S., & Zhyltsov, O. (2022). Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves. In Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), 3288, 1–10. (Scopus).

2. Bessalov, A., Abramov, S., Sokolov, V., & Mazur, N. (2023) CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution. In

Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), 3421, 36–45. (Scopus).

3. Bessalov, A., Abramov, S., Sokolov, V., Skladannyi, P., & Zhyltsov, O. (2023). Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves. In Workshop on Classic, Quantum, and Post-Quantum Cryptography (CQPC), 3504, 12–25. (Scopus).

4. Abramov, S., Bessalov, A., & Sokolov, V. (2023). Properties of Isogeny Graph of Non-Cyclic Edwards Curves. In Workshop on Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II), 3550, 234–239. (Scopus).

5. Abramov, S., Sokolov, V., & Abramov, V. (2024). Research of the Graphic Model of the Points of the Elliptic Curve in the Edward Form. In Workshop on Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II), 3826, 174–181. (Scopus).

6. Абрамов, С.В. (2024). Алгоритм інкапсуляції ключа на кривих Едвардса. На IV Міжнародній науково-практичній інтернет-конференції «Цифрова трансформація фінансової системи України та країн V-4 в умовах євроінтеграції», II, 98–104.

7. Абрамов, С.В. (2024). Дослідження структури графа ізогеній еліптичної кривої Едвардса. На Міжнародній науково-технічній конференції «Інформаційно-комунікаційні технології та кібербезпека» (ІКТК), 200–201.

Особистий внесок здобувача. Дисертація є самостійною науковою працею, в якій висвітлено власні ідеї і розробки автора, що дозволили вирішити поставлені завдання. Робота містить теоретичні та методичні положення і висновки, сформульовані здобувачкою особисто. Використані в дисертації ідеї, положення чи гіпотези інших авторів мають відповідні посилання і використані лише для підкріплення ідей здобувача.

У статті «Randomization of CSIDH Algorithm on Quadratic and Twisted Edwards Curves» опублікованій у співавторстві, внесок Абрамова С.В. полягає в огляді існуючих підходів до вирішення проблеми і обговорення шляхів її вирішення, що загалом складає 35% тексту статті.

У статті «Special Properties of the Point Addition Law for Non-Cyclic Edwards Curves» опублікованій у співавторстві, внесок Абрамова С.В. полягає в аналізі особливих властивостей двох класів квадратичних і скручених кривих Едвардса над простим полем, пов'язаних з їхньою нециклічною структурою і неповнотою закону додавання точок, у створенні моделі точок кривої Едвардса, що загалом складає 40% тексту статті.

У статті «PQC CSIKE Algorithm on Non-Cyclic Edwards Curves» опублікованій у співавторстві, внесок Абрамова С.В. полягає у обговоренні та реалізації ідеї відмови від обчислення ізогенної функції $\varphi(R)$ випадкової точки R, що загалом складає 40% тексту статті.

У статті «Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves» опублікованій у співавторстві, внесок Абрамова С.В. полягає у створенні програмного забезпечення розрахунків і дослідження властивостей системи, що загалом складає 30% тексту статті.

У статті «Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves» опублікованій у співавторстві, внесок Абрамова С.В. полягає у розробці ідеї використання в алгоритмі CSIKE нециклічних кривих Едвардса, створенні програм та розрахунків параметрів моделі алгоритму CSIKE на нециклічних кривих Едвардса, що загалом складає 40% тексту статті.

У статті «CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution» опублікованій у співавторстві, внесок Абрамова С.В. полягає у створенні загальної схеми комбінування модернізованого асиметричного алгоритму на кривих Едвардса із симетричними алгоритмами з автентифікацією, а також створення комп'ютерної моделі комбінованої системи та її програмування, що загалом складає 35% тексту статті.

У статті «Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves» опублікованій у співавторстві, внесок Абрамова С.В. полягає у тому, що зроблено оцінки властивостей для порівняння криптоалгоритмів CSIDH і RCNSE, виконано розрахунки для створення моделі криптосистеми на 4-х степенях ізогеній {3,5,7,37} над полем F_{863} для пари квадратичного кручення з порядками 840 і 888, що загалом складає 30% тексту статті.

У статті «Properties of Isogeny Graph of Non-Cyclic Edwards Curves» опублікованій у співавторстві, внесок Абрамова С.В. полягає у обчислення графу і виявлення закономірностей його ізогеній, що загалом складає 85% тексту статті.

У статті «Research of the Graphic Model of the Points of the Elliptic Curve in the Edward Form» опублікованій у співавторстві, внесок Абрамова С.В. полягає у розрахунку моделі експоненціювання еліптичної кривої, створенні шаблону для обчислення порядку точок і правил реконструкції точок у шаблоні, що загалом складає 70% тексту статті.

Структура та обсяг дисертації. Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел із 76 найменувань на 9 сторінках і 3 додатків. Загальний обсяг роботи становить 161 сторінки, серед яких 149 сторінок – основного тексту, 18 рисунків і 16 таблиць.

Оцінка мови та стилю дисертації. Дисертація написана науковою українською мовою. Стиль викладу матеріалу логічний і послідовний. Зміст роботи повністю висвітлює результати наукових досліджень. Текст роботи має смислову цілісність, послідовність і завершеність, що забезпечує легкість і доступність сприйняття матеріалу.

Дотримання здобувачем академічної доброчесності в дисертації та наукових публікаціях, в яких висвітлено наукові результати дисертації. На підставі вивченого тексту дисертації і наукових публікацій, результатів автоматизованої перевірки на плагіат та їх експертної оцінки, встановлено, що дисертація і наукові публікації виконані самостійно, не містять академічного плагіату, фальсифікації, фабрикації.

Відповідність дисертації вимогам, що представляються до дисертацій на здобуття ступеня доктор філософії. Дисертація Абрамова С.В., на тему

«Моделі та методи підвищення швидкодії алгоритму CSIDH на основі суперсингулярних скручених кривих Едвардса» є завершеним науковим дослідженням, в якому отримано нові обґрунтовані результати. Дисертацію виконано на достатньо високому рівні, її результати мають наукову новизну і практичну значимість. Основні положення дисертації опубліковані в наукових фахових виданнях і міжнародних виданнях, що входять до наукометричних баз Scopus та Web of Science Core Collection та оприлюднювались на міжнародних науково-практичних конференціях. Дисертаційне дослідження відповідає обраній темі, розкриває її суть та підтверджує, що автором повністю вирішено поставлені у роботі завдання.

Рішення:

1. Дисертація Абрамова С.В., на тему «Моделі та методи підвищення швидкодії алгоритму CSIDH на основі суперсингулярних скручених кривих Едвардса», подана на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека, є завершеною, самостійною роботою, що містить науково обґрунтовані результати, актуальність, наукову новизну, теоретичне та практичне значення і відповідає пп. 6–9 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12.01.2022 №44 (зі змінами), наказу Міністерства освіти і науки України від 12.01.2017 №40 «Про затвердження Вимог до оформлення дисертації», затвердженого Міністерством юстиції України 03.02.2017 за №155/30023.

2. Дисертація Абрамова Сергія Вадимовича та наукові публікації, у яких висвітлено наукові результати дисертації, виконано на належному науковому рівні з дотриманням академічної доброчесності.

3. Абрамов Сергій Вадимович на високому рівні оволодів методологією наукової діяльності, набув теоретичних знань, відповідних умінь, навичок та компетентностей. Здобувач вільно володіє матеріалом.

4. Рекомендувати дисертацію Абрамова С.В., на тему «Моделі та методи підвищення швидкодії алгоритму CSIDH на основі суперсингулярних скручених кривих Едвардса» до публічного захисту у разовій спеціалізованій вченій раді для присудження Абрамову С.В. ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека.

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Код ЄДРПОУ 45307965
ВЛАСНИЙ ПІДПИС ЗАСВІДЧУЮ

Голова–
кандидат технічних наук, доцент
завідуючий кафедри інформаційної
та кібернетичної безпеки
імені професора Володимира Бурячка
Київського столичного університету
імені Бориса Грінченка Павло СКЛАДАННИЙ