**ВІДГУК**
**ОФІЦІЙНОГО ОПОНЕНТА**
**доктора технічних наук, професора**
**Козлюк Ірини Олексіївни**
на дисертацію Літави Гжегожа Владислава
«Моделі та засоби підвищення живучості інформаційно-управляючих систем на основі еліптичних кривих»,
подану на здобуття наукового ступеня кандидата технічних наук
за спеціальністю 05.13.06 – інформаційні технології

***Актуальність теми дисертації.*** На сьогоднішній день щораз більше уваги приділяється захисту інформації та конфіденційності. Нехтування додатковими дефіцитами гарантоздатності, такими як інформаційно-управляючі системи (ІУС), може призвести до що п'ятої відмови атомного енергетичного обладнання і що п'ятої аварії космічно-ракетної техніки, з тенденцією їх зростання за останні роки. Цій темі притаманний міжнародний характер та її розгляду присвячено низку міжнародних конференцій, пов'язаних з гарантоздатністю, зокрема з її складовими – живучістю та функціональною безпекою IT: DESSERT, DSN, EDCC, ESREL, SAM, SAFECOMP, тощо. Важливим питанням є дослідження спеціальних режимів функціонування ІУС з точки зору їх живучості, які, у поєднанні з розвитком комплексних інтегрованих дистанційних сенсорів, належать до одного з провідних наукових напрямів найбільших інженерних викликів XXI століття, визначених науковим фондом NSF, а також передбачених до виконання згідно з Постановою Президії НАН України.

Істотним завданням постає оцінювання та підвищення живучості ІУСЕК, а також самих алгоритмів шифрування. Від криптографічних пристроїв вимагається також можливість шифрування та розшифрування в реальному часі. Крім цього, не слід скидати з рахунків одну з основних проблем безпеки, яка зводиться до розв'язання задачі дискретного логарифмування. Кожне збільшення швидкості виконання основних обчислень на ЕК зумовлює скорочення часу, необхідного для знаходження цього логарифму. Одним з основних факторів, який визначає ефективність обчислювальних методів, моделей та технологій не тільки щодо швидкості шифрування/розшифрування, а також непрямо рівень гарантоздатності ECCD і відповідно параметри живучості ІУСЕК, є швидкодія додавання точок на ЕК, від якої безпосередньо залежить час, необхідний для розв'язання дискретного логарифма.

Тому дисертаційна робота Літави Гжегожа Владислава, яка присвячена удосконаленню моделей та засобів ІУС, що базуються на пристроях для виконання криптографічних операцій на ЕК, для підвищення живучості цих систем, є актуальною та має практичне значення.

***Нові наукові результати дисертації, їх новизна, обґрунтованість, достовірність, теоретична та практична цінність.*** Аналіз дисертаційної

роботи здобувача дає змогу зробити висновки, що *новизна отриманих наукових результатів* полягає в тому, що:

1. Удосконалено структурну модель підвищення живучості ІУСЕК з врахуванням дефектів зовнішніх впливів за ознаками ймовірності та детермінованості, що дало змогу створити підґрунтя для проектування ефективних засобів цих систем.

2. Удосконалено технології обчислень на ЕК шляхом заміни множення за модулем в алгоритмі Крестенсона, що дало змогу звести множення до операції додавання, яка відрізняється від відомих новою архітектурою і меншою складністю у порівнянні з підходом, який ґрунтується на традиційному множенні, завдяки чому збільшено швидкість обчислень і прискорено дію алгоритму розв'язання задачі дискретного логарифмування у пристроях ІУСЕК.

3. Вперше одержано модифіковані моделі засобів обчислень на ЕК у пристроях ІУСЕК з врахуванням дефектів зовнішніх впливів на них, що дозволило по-новому визначити розмір кривих, які застосовуються в інтегрованих інформаційних системах, і забезпечити підвищену ефективність засобів протидії потенційним впливам.

4. Вперше, ґрунтуючись на алгоритмі модульного множення в теоретико-числових базисах Радемахера-Крестенсона щодо розв'язання дискретного логарифму, розроблено моделі, технології та структури засобів обчислень на ЕК в ІУСЕК для виконання криптографічних операцій, завдяки чому здійснено верифікацію параметрів живучості ІУСЕК та доведення збільшення його рівня.

*Обґрунтованість і достовірність нових наукових положень, висновків і рекомендацій*, сформульованих у дисертації, підтверджується коректною постановкою задач, науковою обґрунтованістю теоретичних положень, використанням апробованого математичного апарату, опублікованими науковими працями у фахових виданнях та актами впровадження.

*Теоретична цінність результатів дисертації* полягає в тому, що автор отримав результати, які сприяють подальшому розвитку теоретичних і методологічних основ удосконаленню моделей та засобів підвищення живучості інформаційно-управляючих систем на основі еліптичних кривих з врахуванням дефектів зовнішніх впливів за ознаками ймовірності та детермінованості.

*Практична цінність результатів дисертації полягає в тому, що* на отриманій експериментальній базі модельованої атаки на ІУСЕК визначено час захисту засобів в залежності від розміру застосованих кривих, завдяки чому оцінено максимальне зростання ризику в короткостроковій перспективі, ґрунтуючись на особливостях симульованих дефектів впливу і даних щодо підвищення продуктивності нових апаратних рішень. Це також забезпечило вибір оптимальних розмірів ЕК в спеціалізованих рішеннях, де важливим є компроміс між обчислювальною потужністю та рівнем захисту з врахуванням часу, протягом якого даний засіб повинен бути живучим.

Також побудовано паралельну систему, в якій швидкість зростає пропорційно до кількості застосованих програмованих матриць FPGA, здійснено також перенесення і симуляцію функціонування заімплементованої моделі на кластері FPGA (120 компонентів), який базується на програмованій матриці серії Virtex-4.

***Рекомендації щодо застосування одержаних автором дисертації результатів.*** Результати дисертаційної роботи доцільно використати в науково-дослідних та вищих навчальних закладах України та Польщі, які займаються розробкою, дослідженням та впровадженням методів і засобів контролю та управління якістю програмних продуктів, а також підготовкою кадрів у сфері інформаційних технологій. Зокрема, в Тернопільському національному технічному університеті імені Івана Пулюя, Державної вищої професійної школи у Новому Сончі, ТОВ "Шредер".

***Повнота викладу основних результатів дисертації в опублікованих працях.*** Основні наукові результати дисертації досить повно опубліковані у 14 працях. 8 із них – наукові статті, серед яких 6 – статті у наукових фахових виданнях України, 2 наукові статті – у провідних закордонних журналах, які входять до міжнародних наукометричних баз (IEEE, Inspec, Scopus, UlrichsWeb, Index Copernicus, Google Scholar, Baztech, ISI Master Journal List тощо), 2 розділи у закордонній монографії, а також 4 публікації в матеріалах конференцій.

***Мова та стиль дисертації та автореферату***. Робота написана грамотно, а стиль викладених в ній матеріалів досліджень, наукових положень, висновків та рекомендацій в цілому забезпечує доступність та легкість їх сприйняття. Зміст автореферату повністю відображає основні положення дисертації.

***Зауваження та недоліки до тексту дисертації та автореферату***:

1. У параграфі 2.2, сторінка 46 дисертаційної роботи «Порівняльна характеристика моделей виконання арифметичних операцій на еліптичних кривих в задачах живучих інформаційно-управляючих систем» не наведено порівняльного аналізу запропонованих алгоритмів виконання арифметичних операцій із відомими методами у системі числення залишкових класів, що утруднює належну оцінку роботи дисертанта.
2. У дисертації, зокрема, на сторінці 77 рисунок 3.3 «Алгоритм паралельного додавання багатьох чисел» термін алгоритм використано не в класичному його розумінні, автор пропонує своє розуміння, проте не наводить нового означення терміну, не користується стандартним графічним позначенням алгоритму, це додає невизначеності у результатах роботи.
3. Дисертант удосконалив моделі обчислень дискретного логарифма із застосуванням теоретико-числових базисів Радемахера-Крестенсона та паралельного додавання на підставі ρ-методу Полларда. Це безумовно підвищує рівень живучості «інформаційно-управляючої» системи, проте знижує рівень її криптографічної стійкості, оскільки рметод Полларда є найефективнішим засобом криптоаналізу. У дисертації в назві «ро-метод Полларда» доцільно писати його оригінальну назву «ρ-метод Полларда».

4. В праці часто використовується термін «управління», зокрема у темі дисертації, що є калькою чужої мови. Доречно було б скористатись терміном «керування» в його класичному технічному визначенні кібернетичної науки, це дозволило б на практиці розвинути термінологію теорії живучості інформаційних систем курування.
5. В розділах 1 та 2 щодо наведених залежностей та математичних перетворень багато посилань на літературні джерела. Це не погано, але вони заважають виділити, що вже відомо, а що запропоновано автором.

Однак, зазначені вище недоліки не впливають на основні наукові результати і не зменшують високого наукового і практичного рівня дисертації здобувача.

***Відповідність дисертації вимогам ДАК МОНмолодьспорту України.***

Дисертація Літави Гжегожа Владислава є закінченою науковою працею, виконаною здобувачем особисто у вигляді спеціально підготовленого рукопису, що містить висунуті автором для прилюдного захисту науково обгрунтовані теоретичні результати і наукові положення та свідчить про його особистий внесок у науку.

Дисертація Літави Гжегожа Владислава оформлена відповідно до державного стандарту і містить отримані автором нові науково-обгрунтовані результати, які в сукупності розв'язують завдання, що має важливу наукову та технічну спрямованість у сфері інформаційних технологій – розробка моделей та засобів підвищення живучості інформаційно-управляючих систем на основі еліптичних кривих.

**ВИСНОВОК:** Дисертаційна робота Літави Гжегожа Владислава відповідає вимогам пунктів 11, 13, 14 «Порядку присудження наукових ступенів і присвоєння вчених звань» стосовно кандидатських дисертацій, а її автор заслуговує присвоєння йому наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – інформаційні технології.

Професор кафедри телекомунікаційних систем
Національного авіаційного університету
доктор технічних наук, професор
«13» 04 2015 року

І.О. Козлюк

Особистий підпис доктора технічних наук, професора Козлюк Ірини Олексіївни засвідчую.

Учений секретар

О. Варченко

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний авіаційний університет
м. КИЇВ