Голові спеціалізованої вченої ради
К 35.874.02 Львівського державного університету безпеки життєдіяльності
доктору технічних наук, професору, заслуженому працівнику освіти України Раку Юрію Павловичу

79007, м. Львів, вул. Клепарівська, 35

ВІДГУК

офіційного опонента
доктора технічних наук, професора Андрощука Олександра Степановича
на дисертаційну роботу Борзова Юрія Олексійовича
«Інформаційні технології підвищення функціональної безпеки систем обробки інформації критичного застосування», яка подана на здобуття наукового ступеня кандидата технічних наук зі спеціальності 05.13.06 – інформаційні технології

Актуальність. За останній час зростає кількість областей де впроваджуються інформаційні технології. Одна з них це застосування інформаційно-управляючих систем у яких здійснюється обробка інформації критичного застосування. Особливої уваги заслуговують інформаційні технології, які стосуються забезпечення функціональної безпеки, а саме цілісності, надійності та безпеки. Якщо процеси прийняття рішень щодо управління системами критичного застосування включають обробку відеоінформації то спотворення її може призвести до катастрофічних наслідків.

На сьогодні спостерігається відсутність підходів щодо застосування універсальних методів обробки відеоінформації, що поєднують у собі декілька функцій. Це є наслідком відсутності відповідного науково-методичного апарату, тому *актуальність теми дисертаційної роботи* не викликає сумніву.

Пошук нових шляхів вирішення проблеми розробки інформаційних технологій забезпечення функціональної безпеки на основі нових моделей і методів обробки та передачі відеоінформації з урахуванням обчислювальних та

часових ресурсів вимагав від автора дослідження значних зусиль як інформаційно-аналітичного, так і дослідно-експериментального характеру.

Незважаючи на складність теми, здобувач творчо використав кращі доробки зарубіжних вчених у галузі завадостійкого кодування, стиснення, шифрування інформації та підтримки прийняття рішень і виконав роботу на достатньо високому науково-практичному рівні.

Дисертаційну роботу було виконано у відповідності із державною програмою забезпечення пожежної безпеки в Україні на 2012-2015 рр., державним науково-технічним програмам, сформульованим в Законі України "Про науково-технічну діяльність" та в Законі України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки". Робота виконувалася у рамках науково-дослідних робіт:

“Створення навчального макету автоматизованої системи оперативно-диспетчерського управління для підготовки та перепідготовки диспетчерів та керівного складу ОДС” (№ держ. реєстрації 0114U004183),

“Розроблення методичних рекомендацій з організації служби оперативного зв’язку, телекомунікаційних систем та інформаційних технологій в системі ДСНС України” (№ держ. реєстрації 0114U004185),

“Розробка методів і моделей захисту інформаційно-комунікаційних систем і мереж у структурних підрозділах ДСНС України” (№ держ. реєстрації 0114U004275).

Ступінь обґрунтованості наукових положень, висновків і рекомендацій. Достовірність висновків і рекомендацій, сформульованих у дисертації, забезпечена теоретичною обґрунтованістю вихідних положень, кількісним та якісним дослідженням фактичного матеріалу, який автор отримав у процесі дослідження.

Зазначимо, що дисертація Борзова Ю. О. відзначається як за своїм змістом, так і характером викладу основних теоретичних положень. Текст дисертації характеризується науковим викладом, смисловою завершеністю,

цілісністю, що є свідченням високої загальної культури автора, його вміння правильно добирати слова, точно і ясно висловлювати наукову думку.

Слід відмітити ідентичність змісту автореферату й основних положень дисертації.

Достовірність результатів досліджень. У роботі дисертант використовував основні положення теорії інформаційних систем, цифрової обробки зображень, теорії безпеки інформації, теорії чисел, лінійної та булевої алгебр, дискретної математики, топології, математичного аналізу та комп'ютерного моделювання.

Всі основні результати дисертаційного дослідження підтверджуються комп'ютерним моделюванням та адекватністю математичних викладок відповідним експериментам, що підтверджує їх достовірність

Практична цінність роботи. Отримані результати досліджень є основою розробленої програмної бібліотеки, яка призначена для забезпечення функціональної безпеки при передаванні зображень у комп'ютерних мережах на основі протоколів TCP, UDP та Http.

Усі розроблені методи на відміну від існуючих підходів характеризуються достатньою стійкістю і надійністю у порівнянні із криптографічним кодуванням RSA і дають змогу створювати інформаційні технології, які не вимагають для свого функціонування значних обчислювальних ресурсів.

Результати дисертаційних досліджень також використовувались в Головному управлінні ДСНС у Львівській області при розробці та впровадженні системи оперативно-диспетчерського управління (СОДУ) та Системи 112 (акт про використання результатів досліджень від 24 червня 2014 року).

На нашу думку, результати роботи можна використовувати для побудови СППР в інших предметних областях: військовій справі, охороні державного кордону, правопорядку тощо.

Структура та зміст дисертації.

У **вступі** обґрунтовано актуальність теми дисертаційної роботи, сформульована мета і завдання дослідження, розкрито наукову і практичну

цінність отриманих результатів. Наведено відомості про публікації та апробацію результатів дисертаційної роботи.

У **першому розділі** проаналізовано якісні атрибути сучасних систем критичного застосування, виділено характеристики сучасних підходів організації функціональної безпеки в автоматизованих системах критичного застосування, розглянуто принципи побудови засобів функціональної безпеки та проаналізовано проблеми забезпечення стійкості при використанні зображень в телекомунікаційних сеансах методом RSA.

Встановлено базові підходи наукових досліджень у напрямі модифікацій алгоритму RSA для підвищення функціональної безпеки в автоматизованих системах критичного застосування.

Результати аналізу наукових досліджень показали, що найефективнішим напрямом вирішення проблеми підвищення функціональної стійкості автоматизованих систем критичного застосування є розроблення інформаційних технологій на основі інтегрального поєднання елементів алгоритму RSA і операторів зашумлення при створенні стійких методів інформаційного захисту зображень в автоматизованих системах критичного застосування.

У **другому розділі** запропоновано підвищення функціональної безпеки для випадку передавання в комунікаційних сеансах напівтонових зображень, які базуються на використанні елементів алгоритму RSA, побітових операцій, бінарних операторів та функцій зашумлення.

Встановлено, що найпростішим із розроблених методів функціональної безпеки є модифікація методу RSA, яка базується на додатковому використанні побітових операцій.

Для оцінки рівнів втрат та зростання рівня зашумленості використовувались метрики попіксельного порівняння та різниця значень ентропії.

За цими метриками результати практичних експериментів засвідчили відсутність інформаційних втрат, зростання рівня зашумленості та відсутність контурів при середніх значеннях ключів.

Розвитком наведеного методу є додаткове внесення зашумленості в процедуру кодування.

У **третьому розділі** запропоновано методи підвищення функціональної безпеки для випадку передавання комунікаційними каналами повноколірних зображень, які базуються на використанні криптосистем RSA та Ель-Гамаля, порозрядних операцій, бінарних операторів та операторів зашумлення.

Перший метод полягає у використання порозрядних та бінарних операцій над елементами матриці інтенсивностей.

У розділі для сумісного використання порозрядних та побітових операцій наведена схема використання двох рядків матриці зображення.

Використання бінарних операторів при криптографічному кодуванні повноколірних зображень посилюється на підставі введення в процедуру матриці ключів.

Найвищої функціональної стійкості в процесі дисертаційних досліджень вдалось досягти при сумісному використанні криптосистем RSA та Ель-Гамаля.

У **четвертому розділі** запропоновано інформаційну технологію підвищення функціональної безпеки для випадку передавання цифрових зображень в телекомунікаційних процедурах та основні архітектури автоматизованих систем критичного застосування стосовно використання цієї технології.

Суть запропонованої інформаційної технології полягає у появі в технологічному процесі "кодування – комунікація – декодування" етапів вибору алгоритму та контролю результатів роботи процедур функціональної безпеки.

Перший з них полягає у автоматизованому виборі алгоритму кодування в залежності від типу зображень і обмежень, які накладає обчислювальне середовище. Другий етап полягає у перевірці якості результатів кодування через оцінку контурів на закодованому зображенні.

Для реалізації розробленої інформаційної технології в автоматизованих системах критичного застосування виокремлено і модифіковано три типові

архітектури, зокрема: однорангової системи, системи із виділеним сервером та розподіленої систем.

Наукова новизна роботи. Дисертантом розроблено *вперше*:

метод забезпечення необхідного рівня функціональної безпеки систем критичного застосування, який ґрунтується на сумісному використанні систем криптографічного кодування Ель-Гамаля і RSA, що дає можливість підвищити стійкість функціонування інформаційних систем при передаванні в комунікаційних процедурах цифрових зображень із зменшенням витрат.

Отримали подальший розвиток:

метод забезпечення необхідного рівня функціональної безпеки систем критичного застосування у випадку циркуляції в телекомунікаційних сеансах напівтонових зображень із глибиною кольору в 1-2 байти, який ґрунтується на інтегральному поєднанні елементів алгоритму криптографічного кодування RSA та операції зашумлення, що дало можливість збільшити рівень безпеки систем без інформаційних втрат;

метод забезпечення функціональної безпеки на основі алгоритму RSA, який завдяки використанню бінарних операторів забезпечує необхідне значення стійкості та унеможливлює несанкціоноване відтворення методами цифрової оброки сигналів повноколірних зображень із глибиною кольору у 3-4 байти в комунікаційних процесах систем критичного застосування;

Усе це надало можливість *удосконалити* інформаційну технологію забезпечення необхідного рівня функціональної безпеки для випадку передавання комунікаційними каналами напівтонових зображень із глибиною кольору в 1-2 байти, яка базується на використанні модифікованого методу RSA та порозрядних операцій, що дає можливість усунути контури на зображеннях та зменшує витрати обчислювальних ресурсів в програмній реалізації процедур забезпечення функціональної безпеки.

Апробація результатів роботи. Автору роботи вдалося на високому рівні висвітлити основні положення і рекомендації дисертації у наукових фахових виданнях – опубліковано 12 наукових праць, з них: 8 – у фахових

виданнях України з технічних наук (з них 6 входять до міжнародних наукометричних баз), 1 – у закордонному виданні, яке індексується міжнародними наукометричними базами та 3 – у матеріалах міжнародних науково-технічних конференцій.

Зауваження по роботі. Дисертаційне дослідження має завершений характер, проте, оцінюючи його позитивно, вважаємо за потрібне висловити низку зауважень, а саме:

стор. 2 автореферату – не правильно розкривається абревіатура СППР – системи прийняття правильних рішень, не розкрито абревіатуру PSNR;

у першому розділі дисертаційної роботи приділено недостатньо уваги системам обробки саме відеоінформації критичного застосування, аналізу завадостійкого кодування, стисненню відеоінформації, не вказано про показники та критерії функціональної безпеки;

у другому та третьому розділі вказується на переваги розроблених методів, але у четвертому розділі не вказується як в цілому нова інформаційна технологія впливає на функціональну безпеку;

у четвертому розділі (рисунки 8, 9 автореферату) представлені схеми удосконаленої інформаційної технології не містять розроблених автором методів;

слабке обґрунтування (у тому числі експериментальне) деяких результатів. Не описується яким чином здійснювалось порівняння в світі теорії і практики експериментів (умови, обмеження, кількість повторювань тощо);

відсутні посилання на походження деяких висловлювань та математичних виразів (п.п 2.1, 2.2 тощо).

Висловлені зауваження не знижують цінності наукової роботи, її науково-теоретичного та практичного значення. Вона є рукописом, в якому отримано нові науково обґрунтовані результати.

Висновки. За актуальністю теми, а також внеском у науку, ступенем новизни й обґрунтованості дисертаційна робота Борзова Юрія Олексійовича на тему «Інформаційні технології підвищення функціональної безпеки систем

обробки інформації критичного застосування» є цілком завершеним науковим дослідженням. Її зміст відповідає паспорту спеціальності 05.13.06 – інформаційні технології. Вважаю, що дисертаційна робота відповідає всім вимогам до кандидатських дисертацій, зокрема пунктам 9, 11 «Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника», а її автор заслуговує на присвоєння йому наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – Інформаційні технології.

Офіційний опонент
начальник докторантури – головний науковий співробітник
Національної академії Державної прикордонної
служби України імені Богдана Хмельницького,
доктор технічних наук, професор О. С. Андрощук

«23» листопада 2015 р.

Підпис засвідчую:
Начальник відділення контролю та
документального забезпечення О. М. Олошинець

«23» листопада 2015 р.