ВІДГУК

офіційного опонента

на дисертаційну роботу ***Борзова Юрія Олексійовича***

«**Інформаційні технології підвищення функціональної безпеки систем обробки інформації критичного застосування**», що представлена на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – інформаційні технології

Актуальність теми дисертації. На сьогодні, одним із актуальних напрямів технологічного розвитку – є автоматизація діяльності об'єктів підвищеної небезпеки та потенційно небезпечних об'єктів, які, зазвичай, функціонують в online режимах чи режимах реального часу. Визначальною характеристикою цих систем є те, що їх функціонування має значний вплив на ефективність забезпечення життєдіяльності людей. Це висуває все нові вимоги стосовно забезпечення стійкості, надійності та безпеки функціонування таких систем.

У відповідності до цих вимог, виникає потреба у розробленні нових методів, методик, методологій та, на їх основі, програмних алгоритмів, які б забезпечували покращене функціонування різноманітних автоматизованих систем в умовах сучасних потреб та новітніх загроз.

Функціональна безпека є однією із основних складових, на яких базується ефективність функціонування систем критичного застосування. Задача її забезпечення ускладнюється у випадку існування комунікаційних транзакцій різноманітними інформаційними об'єктами, у тому числі цифровими зображеннями. Відповідно, гарантування стійкого, надійного і захищеного передавання зображень комунікаційними каналами, стає елементом забезпечення безпеки обробки інформації в інформаційно-управляючих системах критичного застосування на базі мережевої архітектури.

Специфіка цифрових зображень, як інформаційних суб'єктів комунікаційних сеансів автоматизованих систем, полягає у тому, що атаку на них можна провести у нетиповий спосіб. Цей спосіб полягає у використанні загальновідомих методів цифрової обробки сигналів, які дають змогу отримати більшу інформативність про об'єкт захисту без використання обчислювально витратних математизованих процедур криптографічного взлому.

Тому розроблення нових методів криптографічних кодувань, для випадку цифрових зображень, дає змогу розв'язати актуальну наукову задачу, яка полягає у розробці інформаційних технологій забезпечення функціональної безпеки інформаційно-управляючих систем критичного застосування, які ґрунтуються на комунікаційних процедурах із застосуванням універсальних засобів з метою мінімізації обчислювальних ресурсів в процесах забезпечення надійності, стійкості та безпеки функціонування цих систем.

Ступінь обґрунтованості і достовірності наукових положень, висновків і рекомендацій, сформульованих у дисертації. Аналіз змісту розділів, використаного методологічного та програмно-алгоритмічного інструментарію та способів його застосування, дає підстави зробити висновок про належну обґрунтованість винесених дисертантом на захист основних наукових результатів. Наукові положення, висновки та рекомендації, сформульовані у дисертації, мають добре обґрунтування за рахунок якісно проведеного теоретичного аналізу, підтверджені результатами їх практичного використання, використання відомостей і положень, почерпнутих з сучасної науково-технічної літератури.

Оцінюючи дисертаційну роботу в цілому, слід відзначити новизну запропонованого та реалізованого здобувачем підходу до вирішення поставленої перед ним задачі. Отримані теоретичні результати дозволяють використати їх практично, при забезпеченні функціональної безпеки в різноманітних інформаційних системах, у тому числі в таких, у яких здійснюється обробка інформації критичного застосування.

Достовірність та цінність результатів дисертаційної роботи підтверджена належною практичною їх апробацією та впровадженням.

Наукова новизна одержаних результатів. До найголовніших нових наукових результатів, отриманих дисертантом особисто, можна віднести:

Вперше розроблено:

- 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 глибиною кольору до 4 байт із зменшенням витрат.

Удосконалено:

- 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.

Отримав 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.

Зв'язок з науковими програмами, планами, темами. Дисертаційна робота виконана в рамках навчальних та науково-дослідних робіт, використовувалася у технічних розробках, пов'язаних із розробкою інформаційних технологій забезпечення функціональної безпеки, що ведуться на кафедрах управління проектами, інформаційних технологій та телекомунікацій і управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, зокрема, за держбюджетними темами "Створення навчального макету автоматизованої системи оперативно-диспетчерського управління для підготовки та перепідготовки диспетчерів та керівного складу ОДС" (0114U004183), "Розроблення методичних рекомендацій з організації служби оперативного зв'язку, телекомунікаційних систем та інформаційних технологій в системі ДСНС України" (0114U004185) та "Розробка методів і моделей захисту інформаційно-комунікаційних систем і мереж у структурних підрозділах ДСНС

України" (0114U004275), де здобувачем на основі запропонованих методів було виконано підзадачу забезпечення функціональної безпеки.

Практичне значення отриманих результатів полягає у тому, що розв'язання сформульованих завдань є основою побудови алгоритмів забезпечення функціональної безпеки в системах обробки інформації критичного застосування. Запропонований підхід для системи критичного застосування, проте може використовуватись як у звичайних інформаційних системах так і в задачах персоніфікованої функціональної безпеки.

Особливістю розроблених методів криптографічного кодування є те, що вони усувають контури на цифрових зображеннях при малих значеннях ключів, що призводить до зменшення обчислювальних витрат в комунікаційних сеансах. При цьому, стійкість до несанкціонованого доступу не лише не зменшується, а навпаки зростає у порівнянні із промислово-використовуваними методами. Експериментальні дослідження підтвердили високу ефективність криптографічного кодування на еталонних зображеннях.

Розроблене програмне рішення має модульну структуру, що дозволяє програмні реалізації алгоритмів обробки використати як складові частини у складі автоматизованих систем критичного застосування.

Результати досліджень знайшли впровадження в Головному управлінні ДСНС у Львівській області при розробці та впровадженні системи оперативно-диспетчерського управління (СОДУ) та Системи 112 та у навчальному процесі Львівського державного університету безпеки життєдіяльності на кафедрі управління інформаційною безпекою.

Повнота викладення наукових положень, висновків і рекомендацій в опублікованих працях. Основні результати роботи доповідались та обговорювались на 3 міжнародних наукових конференціях, дві з яких мали спеціалізовані секції по інформаційній та функціональній безпеці. За темою дисертаційної роботи опубліковано 12 друкованих праць, серед них 1 стаття у закордонному виданні (з імпакт фактором), що входить до міжнародних наукометричних баз, 8 статей у наукових фахових виданнях України з технічних наук та 3 публікації у збірниках праць міжнародних наукових конференцій.

Публікації достатньо повно відображають основні результати роботи та зміст дисертації.

Оцінка основного змісту дисертації та її структури. Дисертація є завершеною науково-дослідною роботою. Її структура логічна, містить перелік

умовних скорочень, вступ, чотири розділи, висновки, список використаних джерел та два додатки.

Оформлення дисертації відповідає основним вимогам щодо оформлення дисертацій. Треба відзначити, що в ній у достатньому обсязі наведено графічні та ілюстративні матеріали, чітко зображені формули, акуратно оформлені додатки. В додатках є документи, які підтверджують практичне впровадження наукових розробок здобувача.

У *першому розділі* розглянуто сучасну класифікацію інформаційних систем обробки інформації критичного застосування. Виділено основні проблеми забезпечення функціональної безпеки таких систем. Проведено порівняльний аналіз сучасних методів та технологій криптографічного кодування. На основі проведеного аналізу визначено переваги та недоліки існуючих методів.

За результатами проведеного аналізу, визначено перелік завдань і наукових досліджень, які потрібно виконати для розв'язання наукової задачі, сформульованої у дисертаційній роботі.

У *другому розділі* міститься опис методів 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. Зокрема удосконалено криптографічне кодування за алгоритмом RSA, яке завдяки додатковому використанню побітових операцій, дає змогу нівелювати появу контурів на напівтонових зображеннях і підвищити криптостійкість схеми захисту в цілому.

Розвитком цієї методології є додаткове внесення зашумленості в процедуру кодування. При цьому джерелом зашумленості пропонується використовувати квадратичні оператори, визначені на координатній області самого зображення. Це дозволяє ще більше підняти криптографічну стійкість результатів кодування при незначному зростанні обчислювальних витрат.

Наведено результати порівняльного аналізу роботи цих методів та існуючих.

У *третьому розділі* міститься опис 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.

Зокрема, запропоновано використання бінарних операторів та операторів зашумлення над елементами матриці інтенсивності, що забезпечує високу

стійкість результатів криптографічного кодування зображення колірного формату RGB до несанкціонованого доступу.

Найвищої функціональної стійкості в процесі дисертаційних досліджень, вдалось досягти при сумісному використанні криптосистем RSA та Ель-Гамаля. При цьому, отримано дві методики криптографічного кодування – за одним та за двома рядками матриці зображення. Варто відзначити, що для повноколірних зображень досягається підвищена криптостійкість, а контури починають зникати навіть при дуже малих значеннях ключів. Проте, такі переваги криптографічного кодування, досягаються при зростанні обчислювальних витрат – серед отриманих методів криптографічного кодування сумісне використання елементів криптосистем RSA та Ель-Гамаля є найбільш обчислювально витратним.

Проведено аналіз ефективності роботи розроблених методів порівняно з існуючими. Результати експериментів підтвердили, що використання розроблених методів криптографічного кодування забезпечує досягнення підвищення рівня функціональної безпеки у порівнянні із використанням типових методів.

У *четвертому розділі* представлено опис програмних засобів інформаційної технології підвищення функціональної безпеки для випадку передавання комунікаційними каналами цифрових зображень. Наведено архітектуру програмної реалізації розроблених в дисертаційній роботі методів криптографічного кодування цифрових зображень та структуру програмних модулів і їх логічних зв'язків.

Виділено класи автоматизованих систем критичного застосування, для яких можливе використання розробленої технології. Для проведення практичних експериментів розроблено програмний примітив однорангової автоматизованої системи мережевої архітектури.

Проведено тестування розробленого програмного забезпечення на реальних даних.

Відповідність дисертації та автореферату встановленим вимогам. За своєю структурою, об'ємом і оформленням дисертація та автореферат відповідають вимогам, встановленим до кандидатських дисертацій.

Автореферат за змістом ідентичний основним положенням, що викладені в дисертації, та не містить інформації, яка не відображена в самій роботі.

Стиль викладу матеріалів досліджень, наукових положень і рекомендацій забезпечує їх адекватне і належне сприйняття.

Загальна оцінка роботи. Дисертація та автореферат написані грамотно, послідовно, коректно та мають завершену логічну структуру. Поставлену автором мету досягнуто, сформульовані задачі вирішено, а висновки повністю відображають основний зміст роботи.

Недоліки та зауваження до роботи:

1. Однією із переваг розроблених методів є можливість використання "малих" ключів в процедурах криптографічного кодування процесів забезпечення функціональної безпеки. Тому, доцільним було б для кожного із розроблених методів навести граничні значення, при яких зберігається обчислювальна ефективність побудованих алгоритмів.

2. Оскільки в роботі вирішується проблема підвищення безпеки систем опрацювання інформації, то варто було б розглянути стійкість розглянутих систем до різних типів стеганографічних атак на зображення, які захищаються в комунікаційних процесах.

3. У роботі варто було б навести залежність ефективності розроблених методів криптографічного кодування від типу цифрових зображень та результати порівняння з існуючими.

4. В розробленій автором інформаційній технології не зовсім зрозумілою є реалізація вибору методу криптографічного кодування для різних типів зображень при їх передаванні в комунікаційних сеансах систем критичного застосування.

5. У програмній реалізації алгоритмів відсутня інформація про використання багатопотокових технологій, що ускладнює розуміння ефективності роботи програмних реалізацій алгоритмів в сучасних мережевих процедурах автоматизованих систем критичного застосування.

6. Відсутні вимоги до технічного забезпечення засобів інформаційної технології підвищення функціональної безпеки.

7. На мою думку, назву рис.9 в авторефераті варто замінити "Архітектура програмної реалізації …" на "Структура програмної реалізації …".

8. В авторефераті рис.5б і рис.5в (дисертація – рис.3.3 та рис. 3.4) не є інформативними.

9. В дисертації та авторефераті присутні помилки та описки (автореферат - ст.1, ст.2; дисертація - ст.8 та ін.).

Проте вказані зауваження не знижують загальної позитивної оцінки дисертаційної роботи.

Висновки

Дисертаційна робота Борзова Юрія Олексійовича "Інформаційні технології підвищення функціональної безпеки систем обробки інформації критичного застосування" є завершеною працею, в якій отримані нові науково обґрунтовані результати, що в сукупності вирішують актуальне науково-прикладне завдання розроблення інформаційної технології підвищення функціональної безпеки інформаційно-управляючих систем критичного застосування, які ґрунтуються на комунікаційних процедурах із застосуванням універсальних засобів мінімізації обчислювальних ресурсів в процесах забезпечення надійності, стійкості та безпеки функціонування цих систем.

Автореферат повністю відповідає змісту дисертації й описує суть одержаних результатів та висновків у дисертаційній роботі і оформлений згідно з чинними вимогами, що висуваються до кандидатських дисертацій.

За актуальністю тематики, рівнем виконання, новизною результатів, їх науковим і практичним значенням, обґрунтованістю висновків, дисертаційна робота відповідає вимогам пп. 9, 11, 12 «Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника», що висуваються до кандидатських дисертацій з технічних наук.

Зміст дисертації відповідає спеціальності 05.13.06 – інформаційні технології, а її автор, Борзов Юрій Олексійович, заслуговує присудження наукового ступеня кандидата технічних наук.

Професор кафедри систем автоматизованого проектування
Національного університету
«Львівська політехніка»,
д.т.н., професор В.М. Теслюк

Підпис проф. Теслюка В.М. засвідчую:
Вчений секретар Національного університету
«Львівська політехніка»,
к.т.н., доцент Р.Б. Брилинський