

## АНОТАЦІЯ

*Іванова О.М.* Моделі та методи гібридного маскування даних у процесі моніторингу програмного коду FPGA-компонентів інформаційних систем. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 122 – «Комп'ютерні науки». – Національний університет «Одеська політехніка» Міністерства освіти і науки України, Одеса, 2026.

У **вступі** обґрунтовано актуальність та доцільність дисертаційного дослідження; показано зв'язок роботи з науковими програмами, планами, темами; сформульовано мету та задачі дослідження, наукову новизну та практичне значення одержаних результатів; визначено методи дослідження; зазначено особистий внесок здобувача, наведено дані про апробацію результатів дисертаційних досліджень та публікації.

**В першому розділі** проведено аналіз існуючих підходів, методів та засобів забезпечення моніторингу програмного коду FPGA-компонентів інформаційних систем. Визначено місце FPGA серед сучасних програмно-керованих компонентів комп'ютерних інформаційних систем. Показано, що FPGA використовуються переважно у складі високопродуктивних систем, що обумовлено придатністю структури цих компонентів для природньої організації паралельних обчислень. Це також значною мірою є мотивацією до використання FPGA в складі комп'ютерних інформаційних систем критичного застосування.

Проведено аналіз інцидентів останніх років, пов'язаних зі дестабілізацією роботи технічних об'єктів підвищеного ризику. Встановлено, що найзначнішим чинником збоїв в роботі критично важливих комп'ютерних систем є зловмисне втручання в їх функціонування. Виконано аналіз методів та засобів протидії втручанням в функціонування FPGA-компонентів інформаційних систем. Показано, що одним з найефективніших підходів до протидії втручанням є оперативний

моніторинг стану програмного коду цих компонентів. Виконання моніторингу потребує формування контрольних даних в момент підготовки програмного коду моніторингу, та їх зберігання з метою використання під час виконання актів моніторингу. Показано, що основним способом обходу моніторингу програмного коду для здійснення втручання є фальсифікація контрольних даних, яка найчастіше реалізується в інсайдерський спосіб зсередини організації. Найбільш суттєвими факторами, які обумовлюють можливість втручання визначено спосіб та місце зберігання контрольних даних моніторингу.

Розглянуто існуючі підходи до зберігання контрольних даних систем моніторингу програмного коду. Встановлено, що підходи, які ґрунтуються на збереженні контрольних даних разом з інформаційним об'єктом програмного коду в файлової системі або пам'яті, або які базуються на приєднанні контрольних даних до інформаційного об'єкта програмного коду і зберіганні їх в якості його частини, мають наступні недоліки: очевидність факту виконання моніторингу; доступність еталонних контрольних даних для зчитування, аналізу та можливої фальсифікації. Підходи, в межах яких контрольні дані зберігаються в централізованій базі даних та отримуються з неї в момент виконання процедури моніторингу пов'язані з проблемою організації доступу до цієї бази даних; складністю захисту бази даних від витоків та не зменшують можливість інсайдерського втручання.

Наявні підходи до зберігання контрольних даних, що базуються на стеганографічних методах, мають переваги, які полягають у приховуванні контрольних даних та факту виконання моніторингу, а також забезпечують утворення єдиного цілого між об'єктом програмного коду та контрольними даними. Такі можливості зазначених підходів забезпечені еквівалентними перетвореннями програмного коду. Однак ці підходи мають і недоліки, які полягають у відносно малому доступному обсязі даних, які можна зберегти в стеганографічний спосіб.

Спроби збільшити цей обсяг в межах наявних стеганографічних підходів стикається з *протиріччям* між тим фактом, що програмний код FPGA являє собою точні дані, спотворення яких не є можливим та неможливістю забезпечення достатнього для задач прихованого моніторингу обсягу зберігання даних за рахунок еквівалентних перетворень програмного коду FPGA.

З урахуванням зазначених факторів виконано обґрунтування напрямку досліджень, направлено на збільшення доступного обсягу для замаскованого зберігання контрольних даних в процесі прихованого моніторингу програмного коду FPGA-компонентів комп'ютерних інформаційних систем шляхом розробки моделей та методів гібридного стеганографічного зберігання цих даних що дає змогу *розірвати вказане протиріччя*. В результаті обґрунтування напрямку досліджень сформульовано мету та визначено задачі дисертації.

У **другому розділі** сформульовано твердження, про те, що при реалізації наближеної обробки даних на FPGA-компонентах, ця наближеність переноситься на точно поданий програмний код FPGA-компонентів. Наслідком цього є можливість замаскованого стеганографічного вбудовування в нееквівалентний спосіб (подібне до того, що використовується стосовно інформаційних контейнерів з наближено поданими елементарними одиницями) додаткових даних в точно поданий інформаційний контейнер, яким є програмний код FPGA-компонентів. Це твердження набуло формалізації у вигляді моделей, які виділяють два види надлишкових ресурсів у складі програмного коду FPGA, що можуть бути використані зі метою замаскованого зберігання даних: а) несуттєві блоки LUT в структурі тих осередків FPGA-компонентів, які виконують наближену обробку даних; б) несуттєві розряди програмного коду блоків LUT при виконанні наближеної обробки даних.

*Для визначення множини надлишкових інформаційних ресурсів програмного коду FPGA*, які виникають в процесі виконання наближених обчислень, та можуть бути використані для стеганографічного зберігання

контрольних даних, розроблено модель замаскованого зберігання даних в середовищі програмного коду FPGA-компонентів, яка оснований на використанні нееквівалентних перетворень програмного коду FPGA та враховує особливості виконання наближених арифметичних операцій в середовищі FPGA.

Експериментальне дослідження, проведене в середовищі розробленого програмного забезпечення, яке реалізує запропоновану модель, підтвердило наявність надлишкових інформаційних ресурсів програмного коду FPGA, а також дозволило їх локалізувати та оцінити їх частку в загальному обсязі програмного коду блоків LUT FPGA-проектів. За результатами експериментів отримано верхню оцінку кількості несуттєвих блоків LUT для проектів, що були використані в експерименті, в діапазоні 39.35 % ... 42.52 % та нижню оцінку кількості зазначених блоків в діапазоні 16.67 % ... 29.91 % від загальної кількості блоків LUT в проекті. Експериментально отримано оцінку частки несуттєвих розрядів програмних кодів блоків LUT для обчислювачів, що виконують наближену обробку даних, яка склала для експериментальних проектів 16.8 % ... 26.3 % від сукупної кількості розрядів програмних кодів блоків LUT у відповідних FPGA-проектах.

**Сформульовано перший пункт наукової новизни:** *вперше розроблено модель замаскованого зберігання даних в середовищі програмного коду FPGA-компонентів, яка оснований на використанні нееквівалентних перетворень програмного коду FPGA та враховує особливості виконання наближених арифметичних операцій в середовищі FPGA, що дозволяє визначити множину надлишкових інформаційних ресурсів, які виникають в процесі виконання таких обчислень, та можуть бути використані для прихованого зберігання контрольних даних.*

**Для збільшення обсягу, доступного для прихованого зберігання додаткових даних** в середовищі програмного коду FPGA-компонентів та необхідного в задачах моніторингу характеристик безпеки програмного

коду FPGA, розроблено метод нееквівалентного замаскованого зберігання даних в середовищі програмного коду FPGA-компонентів, який характеризується використанням надлишковості програмного коду FPGA, яка виникає при виконанні наближеної обробки даних.

Виконано експериментальне дослідження функціонування реалізації запропонованого методу. Додатковий обсяг для замаскованого зберігання даних, забезпечений запропонованим методом склав для виділеного надлишкового стеганографічного ресурсу програмних кодів несуттєвих блоків LUT в експериментальних FPGA-проектах за верхньою оцінкою: від 12 до 145 біт при використанні з метою замаскованого збереження даних тільки одного розряду програмного коду несуттєвих блоків LUT та від 192 до 2320 біт при використанні всіх розрядів програмного коду зазначених блоків; та за нижньою оцінкою від 5 до 102 біт при використанні одного розряду програмного коду блоків LUT та від 80 до 1632 біт при використанні всіх розрядів програмного коду зазначених блоків. Для експериментальних FPGA-проектів кількість несуттєвих розрядів програмного коду блоків LUT склала від 89 до 690.

Запропоновані та експериментально дослідженні в даному розділі дисертації надлишкові інформаційні ресурси додають до обсягів прихованого зберігання даних в програмному коді FPGA, забезпечених відомими методами, додаткові обсяги для зберігання контрольних даних, що дає змогу збереження контрольних даних більшої кількості видів оперативного моніторингу та додає варіативності у виборі розміру виходу хеш-функцій, використовуваних для отримання контрольних даних.

**Сформульовано другий пункт наукової новизни:** *вперше розроблено метод нееквівалентного замаскованого зберігання даних в середовищі програмного коду FPGA-компонентів, що характеризується використанням надлишковості програмного коду FPGA, яка виникає при виконанні наближених арифметичних операцій, що дозволяє збільшити*

обсяг, доступний для прихованого зберігання контрольних даних в задачах моніторингу характеристик безпеки програмного коду FPGA.

В **третьому розділі** дисертації запропоновано підходи до гібридного замаскованого зберігання даних в програмному коді FPGA, які поєднують еквівалентні та нееквівалентні перетворення програмного коду для вбудовування даних, а також дають можливість застосування відновної обфускації в процесі вбудовування додаткових даних в програмний код.

*Для збільшення обсягу контрольних даних, які можуть бути приховано вбудованими в програмний код FPGA, не збільшуючи здатність традиційних методів стегоаналізу до виявлення цих даних в програмному коді*, розроблено метод гібридного замаскованого зберігання контрольних даних в середовищі програмного коду FPGA, який відрізняється поєднанням еквівалентного та нееквівалентного підходів до перетворення програмного коду FPGA, а також поєднанням процесів стеганографічного вбудовування та відновної обфускації даних.

Гібридність методу, полягає в двох видах комбінування властивостей відомого еквівалентного підходу та, запропонованого в даній роботі, нееквівалентного підходу до замаскованого зберігання контрольних даних в програмному коді FPGA:

1) комбінування стеганографічних ресурсів, забезпечених еквівалентними та нееквівалентними перетвореннями програмного коду FPGA, для досягнення потрібного обсягу даних в середовищі програмного коду та послідовному виділенні цих ресурсів для мінімізації обчислювальної складності їх застосування;

2) комбінування стеганографічного вбудовування (з використанням обох підходів) даних в програмний код FPGA та зворотної (відновної) обфускації програмного коду FPGA, базованої на моделі еквівалентних перетворень, та призначеної для ускладнення стегоаналізу і виявлення прихованих в програмному коді даних.

Виконано експериментальне дослідження ефективності розробленого гібридного методу для задач прихованого зберігання контрольних даних в процесі моніторингу програмного коду FPGA-компонентів. Для експериментальних FPGA проєктів збільшення обсягу потенційно доступних додаткових даних за рахунок використання надлишкових інформаційних ресурсів несуттєвих блоків LUT при застосуванні швидкого способу локалізації цих блоків склало від 7,1% до 40,8% та в середньому 22,6%, а при застосуванні базового способу локалізації зазначене збільшення склало від 9,2% до 73,4% та в середньому 34,0%.

Збільшення обсягу потенційно доступних додаткових даних за рахунок використання крім цього також надлишкових інформаційних ресурсів несуттєвих розрядів суттєвих блоків LUT при застосуванні швидкого способу локалізації цих блоків склало від 31,7% до 138,9% та в середньому 93,7%. При застосуванні базового способу локалізації зазначене збільшення склало від 33,8% до 157,9% та в середньому 105,1%.

Виконано експериментальну оцінку ймовірності виявлення відомими методами та засобами стегааналізу наявності даних, приховано вбудованих в програмний код FPGA, запропонованим гібридним методом. Оцінка ймовірності наявності додаткових даних при їх вбудовуванні гібридним методом без виконання етапу відновної обфускації збільшується в середньому на 2,31%, порівняно з застосуванням еквівалентного підходу, та зменшується на 6,43% в разі виконання відновної обфускації.

***Сформульовано третій пункт наукової новизни:*** *вперше розроблено метод гібридного замаскованого зберігання даних в середовищі програмного коду FPGA, який відрізняється поєднанням еквівалентного та нееквівалентного підходів до перетворення програмного коду FPGA, а також поєднанням процесів стегаграфічного вбудовування та відновної обфускації даних, що дозволяє збільшити обсяг контрольних даних, які можуть бути приховано вбудованими в програмний код FPGA, не збільшуючи при цьому здатність традиційних методів стегааналізу до виявлення цих даних в програмному коді.*

*Для введення можливості балансування між обсягом частини програмного коду, яка модифікується в результаті замаскованого вбудовування даних та ефективним обсягом стеганографічного контейнера, потрібним для збереження контрольних даних, розроблено метод формування стеганографічного ключа для прихованого збереження контрольних даних в програмному коді FPGA, який відрізняється можливістю адаптації до структури зв'язків між елементарними одиницями FPGA та до необхідного обсягу контрольних даних. Метод може бути застосований в якості доповнення як до традиційних методів стеганографічного вбудовування даних в програмний код FPGA, так і до гібридного методу.*

Виконано експериментальне дослідження ефективності розробленого методу формування стеганографічного ключа, які показали середнє збільшення на 22,8% ефективного обсягу цифрового водяного знака, який містить контрольні дані та може бути приховано вбудований в програмний код FPGA.

*Сформульовано четвертий пункт наукової новизни: дістав подальшого розвитку метод формування стеганографічного ключа для замаскованого збереження даних в програмному коді FPGA, який відрізняється можливістю адаптації до структури зв'язків між елементарними одиницями FPGA та до необхідного обсягу контрольних даних, що дозволяє виконувати балансування між обсягом частини програмного коду, яка модифікується в результаті вбудовування даних та ефективним обсягом стеганографічного контейнера, потрібним для збереження контрольних даних.*

В четвертому розділі дисертаційної роботи розроблено підсистему гібридного замаскованого зберігання контрольних даних в складі інформаційної системи прихованого моніторингу програмного коду FPGA-компонентів. Сформульовано мету та задачі функціонування зазначеної підсистеми у складі головної інформаційної системи.

Специфіковано сукупність інформаційних потоків підсистеми, яка визначає вхідні та вихідні дані, інформаційну взаємодію з іншими компонентами систем, зовнішнім програмним середовищем та користувачами. Визначено перелік функціональних та нефункціональних вимог до підсистеми. Для розроблюваного програмного забезпечення створено діаграми логічного уявлення, розгортання, визначено структуру програмного проєкту та виконано аналіз програмного коду, що в сукупності формалізувало архітектуру підсистеми. Проведено комплексне тестування розробленої підсистеми, що довело її готовність до використання в складі інформаційної системи прихованого моніторингу програмного коду FPGA-компонентів.

Запропоновані в дисертаційній роботі методи та розроблені на їх основі програмні засоби були впроваджені в науково-дослідницьку діяльність та навчальний процес Національного університету «Одеська політехніка».

*Ключові слова:* зберігання інформації в комп'ютерних системах; доступу до інформації в комп'ютерних системах; замасковане зберігання даних, прихований моніторинг програмного коду FPGA-компонентів інформаційних систем, обробка наближених даних, обфускація програмного коду.

### **Список публікацій здобувача за темою дисертації**

#### ***Праці, які відображають основні наукові результати дисертації***

1. Антощук С.Г., Іванова О.М. Швидка локалізація осередків програмного коду FPGA, придатних для стеганографічного зберігання додаткових даних. *Вісник Херсонського національного технічного університету*. Херсон, 2025. № 4 (95) Ч. 3. С. 9 – 14. DOI: <https://doi.org/10.35546/kntu2078-4481.2025.4.3.1>. Видання включено до переліку наукових фахових видань України (категорія Б).

[https://journals.kntu.kherson.ua/index.php/visnyk\\_kntu/article/view/1265/1215](https://journals.kntu.kherson.ua/index.php/visnyk_kntu/article/view/1265/1215)

2. Антощук С.Г., Іванова О.М. Метод формування стега-ключа для збільшення обсягу прихованого зберігання даних в середовищі програмного коду FPGA. *Вісник Херсонського національного технічного університету*. Херсон, 2025. № 1 (92). С. 9 – 16. DOI: <https://doi.org/10.35546/kntu2078-4481.2025.1.2.1>. Видання включено до переліку наукових фахових видань України (категорія Б).

[https://journals.kntu.kherson.ua/index.php/visnyk\\_kntu/article/view/836/803](https://journals.kntu.kherson.ua/index.php/visnyk_kntu/article/view/836/803)

3. Антощук С.Г., Іванова О.М. Підхід до збільшення обсягу прихованого зберігання даних, призначених для моніторингу FPGA-компонентів комп'ютерних систем. *Вчені записки Таврійського національного університету. Серія: «Технічні науки»*. Київ, 2023. Том 34 (73), № 6. DOI: <https://doi.org/10.32782/2663-5941/2023.6/08>. Видання включено до переліку наукових фахових видань України (категорія Б).

[https://www.tech.vernadskyjournals.in.ua/journals/2023/6\\_2023/8.pdf](https://www.tech.vernadskyjournals.in.ua/journals/2023/6_2023/8.pdf)

4. Іванова О.М., Дрозд О.В., Защолкін К.В., Кузнєцов М.О. Підхід до нееквівалентного стеганографічного вбудовування додаткових даних в програмний код блоків LUT FPGA. *Вісник Кременчуцького національного університету імені М. Остроградського*. Кременчук, 2021. № 6 (131). С. 60–65. DOI: <https://doi.org/10.30929/1995-0519.2021.6.60-65>. Видання включено до переліку наукових фахових видань України (категорія Б).

[https://visnikkrnu.kdu.edu.ua/statti/2021\\_6\\_2021-6-60-65.pdf](https://visnikkrnu.kdu.edu.ua/statti/2021_6_2021-6-60-65.pdf)

5. Zashcholkin K., Drozd O., Antoshchuk S., Ivanova O., Sachenko O. Steganographic Resources of FPGA-based Systems for Approximate Data Processing. *CEUR-WS*. 2021. Vol. 2864. P. 324-333. *Наукове періодичне іноземне видання, Німеччина, ISSN 1613-0073*. Видання включено до наукометричної бази **SCOPUS**

<https://ceur-ws.org/Vol-2864/paper28.pdf>

6. Zashcholkin K., Drozd O., Ivanova O., Shaporin R., Kuznietsov M. An Approach to Stego-Container Organization in FPGA Systems for Approximate Data Processing. *CEUR-WS*. 2021. Vol. 2853. P. 527–536. *Наукове періодичне іноземне видання, Німеччина, ISSN 1613-0073. Видання включено до наукометричної бази SCOPUS*

<https://ceur-ws.org/Vol-2853/paper55.pdf>

7. Ivanova O., Drozd O., Zashcholkin K., Sulima Y. Combined Use of Equivalent and Non-Equivalent Transformations of FPGA Program Code to Embedding Additional Security Data. *IEEE East-West Design and Test Symposium (EWDTS)*. 2021. P. 191 – 195. DOI: <https://doi.org/10.1109/EWDTS52692.2021.9580984>. *Наукове періодичне іноземне видання, США, ISSN: 2373-826X. Видання включено до наукометричної бази SCOPUS*

<https://ieeexplore.ieee.org/abstract/document/9580984>

8. Zashcholkin K., Drozd O., Ivanova O., Bykovyy P. Formation of the Interval Stego Key for the Digital Watermark Used in Integrity Monitoring of FPGA-based Systems. *CEUR-WS*. 2020. Vol. 2623. P. 267 – 276. *Наукове періодичне іноземне видання, Німеччина, ISSN 1613-0073. Видання включено до наукометричних баз SCOPUS та Web of Science Core Collection*

<https://ceur-ws.org/Vol-2623/paper23.pdf>

9. Zashcholkin K., Drozd O., Shaporin R., Ivanova O., Drozd M. Co-Embedding Additional Security Data and Obfuscating Low-Level FPGA Program Code. *IEEE East-West Design and Test Symposium (EWDTS)*. 2020. P. 115 – 119. DOI: <https://doi.org/10.1109/EWDTS50664.2020.9225111>. *Наукове періодичне іноземне видання, США, ISSN: 2373-826X. Видання включено до наукометричної бази SCOPUS*

<https://ieeexplore.ieee.org/document/9225111>

10. Патент на винахід № 122276 Україна, МПК G06F 11/263 (2006.01), G06F 7/544 (2006.01). Програмований пристрій для обчислення

логічної функції N змінних / К.В. Зацолкін, О.В. Дрозд, Р.О. Шапорін, О.М. Іванова, Ю.В. Дрозд; заявник Одеський національний політехнічний університет. – № а201811671; заявлено 27.11.2018; опубліковано 12.10.2020; Бюл. № 19/2020.

<https://sis.nipo.gov.ua/uk/search/detail/1458192>

### ***Наукові праці апробаційного характеру***

11. Антощук С.Г., Іванова О.М., Зацолкін К.В. Стеганографічне вбудовування додаткових даних в програмний код мікросхем FPGA. *Перспективні напрямки сучасної електроніки, інформаційних і комп'ютерних систем, MEICS-2023*: матеріали VIII Всеукраїнської науково-практичної конференції. Дніпро, 2023.

[https://www.dnu.dp.ua/docs/ndc/2023/materiali%20konf/25\\_MEICS-2023.pdf](https://www.dnu.dp.ua/docs/ndc/2023/materiali%20konf/25_MEICS-2023.pdf)

12. Іванова О.М., Дрозд О.В., Зацолкін К.В. Особливості стеганографічного нееквівалентного вбудовування цифрових водяних знаків в програмний код FPGA. *Інформатика, управління та штучний інтелект, ІУШІ-2021*: тези VIII Міжнародної науково-технічної конференції. Харків, 2021.

[https://web.kpi.kharkov.ua/ai/wp-content/uploads/sites/249/2024/10/TEZY\\_YUYU\\_2021.pdf](https://web.kpi.kharkov.ua/ai/wp-content/uploads/sites/249/2024/10/TEZY_YUYU_2021.pdf)

13. Іванова О.М., Михайлов Д.О., Зацолкін К.В. Підхід до 3D стеганографічного вбудовування даних та його програмна реалізація. *Сучасні інформаційні технології, МІТ-2021*: матеріали XI Міжнародної наукової конференції. Одеса, 2021. С. 36 – 37.

### ***Публікації, які додатково висвітлюють результати дисертації***

14. Drozd O., Maevsky D., Maevskaya O., Martynyuk O., Parkhomenko A., Gladkova O., Drozd M., Ivanova O., Surkov S., Zashcholkin K. Internet of Things for Smart Building and City. Ministry of Education and Science of Ukraine, 2019. 156 p.

[https://aliot.eu.org/wp-content/uploads/2020/01/ALIOT\\_ITM2\\_IoT-for-Smart-Build-and-City\\_web.pdf](https://aliot.eu.org/wp-content/uploads/2020/01/ALIOT_ITM2_IoT-for-Smart-Build-and-City_web.pdf)

## ABSTRACT

*Ivanova O.M.* Models and methods for hybrid data masking in the process of monitoring the program code of FPGA-components of information systems. – Qualification scientific work in the form of manuscript.

Thesis for the PhD degree in specialty 122 Computer science. – Odesa Polytechnic National University, Ministry of Education and Science of Ukraine, Odesa, 2026.

The **introduction** substantiates the relevance and practicability of the dissertation research; demonstrates the connection between the work and scientific programs, plans, and topics; formulates the purpose and objectives of the research, the scientific novelty and practical significance of the results obtained; defines the research methods; the applicant's personal scientific contribution is indicated, data on the testing of the dissertation research results are provided, as well as information on publications.

The **first chapter** analyzes existing approaches, methods, and means of monitoring the program code of FPGA-components in information systems. The role of FPGAs among modern software-controlled components of computer information systems has been identified. It is shown that FPGAs are mainly used in high-performance computer systems, which is due to the suitability of the structure of these chips for the natural organization of parallel computing. This is also a significant motivation for the use of FPGA in critical computer systems.

An analysis of incidents in recent years related to the destabilization of high-risk technical facilities has been conducted. It has been established that the most significant factor in the failure of critical computer systems is malicious interference in their operation. An analysis of methods and means of counteracting interference in the operation of FPGA-components of computer systems has been carried out. It has been shown that one of the most effective approaches to countering interference is the operational monitoring of the state of the software code of these components. Monitoring requires the formation of

control data at the time the program code is prepared for monitoring, and the storage of that data for use during the execution of monitoring acts. It is shown that the main way to bypass program code monitoring for the purpose of interference is to falsify control data, which is most often done by insiders from within the organization. The most significant factor determining the possibility of interference is the method of storing control data.

Existing approaches to storing control data for program code monitoring systems are considered. It has been established that approaches based on storing control data together with the program code information object in a file system or memory, or based on attaching control data to the program code information object and storing it as part of it, have the following disadvantages: the obviousness of the fact that monitoring is being performed; the availability of reference control data for reading, analysis, and possible falsification. Approaches in which control data is stored in a centralized database and retrieved from it at the time of monitoring are associated with the problem of organizing access to this database; the complexity of protecting the database from leaks; and do not reduce the possibility of insider interference.

Existing approaches to storing control data based on the steganographic approach have advantages that consist in hiding control data and the fact of monitoring, as well as ensuring the creation of a single whole between the object of the program code and the control data. These capabilities of the above approaches are provided by equivalent transformations of the program code. However, these approaches also have disadvantages, which consist in the relatively small volume of data that can be stored in a steganographic way.

Attempts to increase this volume within the limits of existing steganographic approaches are faced with a contradiction between the fact that FPGA program code represents exact data, the distortion of which is impossible, and the impossibility of ensuring sufficient data storage volume for hidden monitoring tasks by means of equivalent transformations of FPGA program code.

Taking into account the above factors, the research direction aimed at increasing the available masked storage capacity for control data in the process of hidden monitoring of the program code of FPGA components of computer systems was justified by developing models and methods of hybrid steganographic storage of these data, which makes it possible to resolve the above contradiction. As a result of justifying the research direction, the objective of the thesis was formulated and its tasks were defined.

The **second chapter** formulates the statement that when implementing approximate data processing on an FPGA, this approximation is transferred to the exactly specified FPGA program code. The result is the possibility of masked embedding in a non-equivalent way (similar to that used for information containers with approximately presented elementary units) of additional data into a exactly specified information container, which is the FPGA program code. This statement has been formalized in the form of models that identify two types of redundant resources in the FPGA program code that can be used for steganographic purposes: a) insignificant LUT units in the structure of compute units that perform approximate data processing; b) insignificant bits of the LUT unit program code when performing approximate data processing.

*To identify a set of redundant information resources in FPGA program code* that arise during the execution of approximate calculations and can be used for steganographic storage of control data, a model of masked data storage in the FPGA component program code environment has been developed, which is based on the use of non-equivalent transformations of the FPGA program code and takes into account the peculiarities of performing approximate arithmetic operations in the FPGA environment.

An experimental research carried out in the environment of the developed software, which implements the proposed model, confirmed the presence of redundant information resources in the FPGA program code, and also allowed to localize them and estimate their share in the total volume of the program code of FPGA-projects. The results of the experiments obtained an upper estimate of the number of insignificant LUT units for experimental projects in the range of

39,35% to 42,52% and a lower estimate of the number of these units in the range of 16,67% to 29,91% of the total number of LUT units in the project. An estimate of the proportion of insignificant bits of LUT block program codes for computing units performing approximate data processing was also obtained experimentally, which amounted to 16,8% to 26,3% of the total number of bits of LUT unit program codes for experimental projects.

***The first point of scientific novelty has been formulated:*** a model of masked data storage within the FPGA program code environment has been developed, which is based on the use of non-equivalent transformations of the FPGA program code and takes into account the peculiarities of performing approximate arithmetic operations in the FPGA environment, This allows us to identify a set of redundant information resources that arise in the process of performing such calculations and can be used for hidden storage of control data.

***To increase the volume available for hidden storage of additional data*** in the FPGA program code environment and required for monitoring the security characteristics of FPGA program code, a method of non-equivalent masked data storage within the FPGA program code environment has been developed, which is characterized by the use of FPGA program code redundancy that arises during approximate data processing.

An experimental study of the results of the proposed method's implementation was conducted. The additional volume for masked data storage provided by the proposed method amounted to the following upper estimates for the allocated excessive steganographic resource of software codes of insignificant LUT units of experimental FPGA projects: from 12 to 145 bits when used for steganographic data storage of only one bit of the program code of insignificant LUT units, and from 192 to 2320 bits when using all bits of the program code of these units; and, according to the lower estimate, from 5 to 102 bits when using one bit of the LUT unit program code and from 80 to 1632 bits when using all bits of the program code of the specified blocks. For experimental FPGA projects, the number of non-essential bits of the LUT unit program code ranged from 89 to 690.

The redundant information resources proposed and experimentally researched in this chapter of the thesis add to the volume of hidden data storage in the FPGA program code, provided by known methods, additional resources for storing control data, which allows for the storage of control data for a greater number of types of operational monitoring and adds variability in the selection of the output size of hash functions used to obtain control data.

*The second point of scientific novelty is formulated:* a method of non-equivalent masked data storage in the FPGA program code environment has been developed, which is characterized by the use of redundancy in the FPGA program code, which arises when performing approximate arithmetic operations, allowing to increase the volume available for hidden storage of additional data in tasks of monitoring the security characteristics of FPGA program code.

The **third chapter** of the thesis proposes approaches to hybrid masked data storage in FPGA program code, which combine equivalent and non-equivalent transformations of program code during embedding, and also enable the use of recoverable obfuscation in the process of embedding additional data into program code.

*To increase the volume of control data that can be hidden in the FPGA program code without increasing the ability of traditional steganalysis methods to detect this data in the program code,* a method of hybrid masked storage of control data in the FPGA program code environment has been developed. This method is distinguished by a combination of equivalent and non-equivalent approaches to the transformation of FPGA program code, as well as a combination of steganographic embedding and data recoverable obfuscation processes.

The hybrid nature of the method consists of two types of combining the properties of the known equivalent approach and the non-equivalent approach proposed in this thesis for masked storage of control data in FPGA program code:

1) combining steganographic resources provided by equivalent and non-equivalent transformations of FPGA program code to achieve the required

volume of data in the program code environment and sequentially allocating these resources to minimize the computational complexity of their application;

2) combining steganographic embedding (using both approaches) of data into FPGA program code and reversible (recoverable) obfuscation of FPGA program code based on a model of equivalent transformations and designed to complicate steganalysis and detection of data hidden in program code.

An experimental research was carried out to evaluate the effectiveness of the developed hybrid method for hidden steganographic storage of control data in the process of monitoring FPGA program code. For experimental FPGA projects, the increase in the volume of potentially available additional data due to the use of the stego-resource of insignificant LUT units when applying a fast method of localizing these units ranged from 7,1% to 40,8% and averaged 22,6%, and when using the basic localization method, the increase ranged from 9,2% to 73,4% and averaged 34,0%.

The increase in the volume of potentially available additional data due to the use of redundant information resources of insignificant bits of significant LUT units when applying the fast method of localizing these units ranged from 31,7% to 138,9% and averaged 93,7%. By using the steganographic resource of insignificant bits of significant LUT units when applying the basic localization method, the increase ranged from 33,8% to 157,9% and averaged 105,1%.

An experimental assessment was performed of the probability of detecting, using known methods and means of steganalysis, the presence of data embedded in the FPGA program code using the proposed hybrid method. The probability of additional data being present when embedding using the hybrid method without performing the recoverable obfuscation stage increases by an average of 2,31% compared to using an equivalent approach, and decreases by 6,43% when performing the recoverable obfuscation stage.

***The third point of scientific novelty has been formulated:*** a method of hybrid masked storage of control data in the FPGA program code environment has been developed, which is distinguished by a combination of equivalent and

non-equivalent approaches to the transformation of FPGA program code, as well as a combination of steganographic embedding and recoverable obfuscation of control data, which allows increasing the volume of control data that can be hidden embedded in FPGA program code without increasing the ability of traditional steganalysis methods to detect this data in the program code.

*To provide a balance between the volume of program code modified as a result of steganographic data embedding and the effective volume of the steganographic container* a method for forming a steganographic key for hidden storage of control data in FPGA program code has been developed, which is distinguished by its ability to adapt to the structure of connections between elementary FPGA units and to the required volume of control data. The method can be applied as a supplement to both traditional methods of steganographic data embedding in FPGA program code and to the hybrid method.

An experimental research was carried out to evaluate the effectiveness of the developed method of steganographic key formation, which showed an average increase of 22,8% in the effective volume of the digital watermark containing control data and can be hidden embedded in the FPGA program code.

*The fourth point of scientific novelty has been formulated:* the method of forming a steganographic key for hidden storage of control data in the FPGA program code has been further developed, which is distinguished by its ability to adapt to the structure of connections between elementary FPGA units and to the required volume of control data, allowing for a balance between the volume of the part of the program code that is modified as a result of data embedding and the effective volume of the steganographic container required to store control data.

The **fourth chapter** of the thesis develops a subsystem for hybrid masked storage of control data as part of an information system for hidden monitoring of FPGA program code. The purpose and objectives of the subsystem's functioning as part of the main information system are formulated.

A set of information flows of the subsystem is specified, which defines the input and output data of the subsystem, its information interaction with other

system components, the external software environment, and users. A list of functional and non-functional requirements for the subsystem has been defined. Diagrams of the logical representation of the subsystem under development and its deployment have been developed, the structure of the software project has been determined, and an analysis of the software code has been performed, which together formalized the architecture of the subsystem. Comprehensive testing of the developed subsystem has been carried out, proving its readiness for use as part of an information system for hidden monitoring of FPGA software code.

The methods proposed in the dissertation and the software tools developed based on them have been applied in research activities and academic courses at Odessa Polytechnic National University.

*Keywords:* information storage in computer systems; access to information in computer systems; masked data storage, hidden monitoring of FPGA-components program code, approximate data processing, program code obfuscation.

### **List of publications**

#### ***Publications where the main scientific results of the dissertation are published***

1. Antoschuk S., Ivanova O. Fast localization of FPGA program code elements suitable for steganographic storage of additional data. *Visnyk of Kherson National Technical University*. Kherson, 2025. N 4 (95). P. 3. P. 9 – 14. DOI: <https://doi.org/10.35546/kntu2078-4481.2025.4.3.1>. *The publication is included in the list of scientific professional publications of Ukraine (category B).*

[https://journals.kntu.kherson.ua/index.php/visnyk\\_kntu/article/view/1265/1215](https://journals.kntu.kherson.ua/index.php/visnyk_kntu/article/view/1265/1215)

2. Antoschuk S., Ivanova O. The interval stego-key method for increasing the volume of hidden data storage in the environment of FPGA chips program code. *Visnyk of Kherson National Technical University*. Kherson, 2025. № 1 (92). C. 9 – 16. DOI: <https://doi.org/10.35546/kntu2078-4481.2025.1.2.1>. *The*

*publication is included in the list of scientific professional publications of Ukraine (category B).*

[https://journals.kntu.kherson.ua/index.php/visnyk\\_kntu/article/view/836/803](https://journals.kntu.kherson.ua/index.php/visnyk_kntu/article/view/836/803)

3. Antoschuk S.H., Ivanova O.M. Approach to increasing the volume of hidden storage of control data for monitoring FPGA components of computer systems. *Scientific Notes of the Tavria National University. Series: "Technical Sciences"*. Kyiv, 2023. Vol. 34 (73), No 6. DOI: <https://doi.org/10.32782/2663-5941/2023.6/08>. *The publication is included in the list of scientific professional publications of Ukraine (category B).*

[https://www.tech.vernadskyjournals.in.ua/journals/2023/6\\_2023/8.pdf](https://www.tech.vernadskyjournals.in.ua/journals/2023/6_2023/8.pdf)

4. Ivanova O.M., Drozd O.V., Zashcholkin K.V., Kuznietsov M.O. An approach to non-equivalent steganographic embedding of additional data into the program code of FPGA LUT units. *Transactions of Kremenchuk Mykhailo Ostrohradskyi National University*. Kremenchuk, 2021. No 6 (131). P. 60–65. DOI: <https://doi.org/10.30929/1995-0519.2021.6.60-65>. *The publication is included in the list of scientific professional publications of Ukraine (category B).*

[https://visnikkrnu.kdu.edu.ua/statti/2021\\_6\\_2021-6-60-65.pdf](https://visnikkrnu.kdu.edu.ua/statti/2021_6_2021-6-60-65.pdf)

5. Zashcholkin K., Drozd O., Antoshchuk S., Ivanova O., Sachenko O. Steganographic Resources of FPGA-based Systems for Approximate Data Processing. *CEUR-WS*. 2021. Vol. 2864. P. 324-333. *Scientific periodical foreign issue, Germany, ISSN 1613-0073. The publication is included in the scientometric base SCOPUS*

<https://ceur-ws.org/Vol-2864/paper28.pdf>

6. Zashcholkin K., Drozd O., Ivanova O., Shaporin R., Kuznietsov M. An Approach to Stego-Container Organization in FPGA Systems for Approximate Data Processing. *CEUR-WS*. 2021. Vol. 2853. P. 527–536. *Scientific periodical foreign issue, Germany, ISSN 1613-0073. The publication is included in the scientometric base SCOPUS*

<https://ceur-ws.org/Vol-2853/paper55.pdf>

7. Ivanova O., Drozd O., Zashcholkin K., Sulima Y. Combined Use of Equivalent and Non-Equivalent Transformations of FPGA Program Code to Embedding Additional Security Data. *IEEE East-West Design and Test Symposium (EWDTS)*. 2021. P. 191 – 195. DOI: <https://doi.org/10.1109/EWDTS52692.2021.9580984>. 9580984. *Scientific periodical foreign issue, USA, ISSN: 2373-826X. The publication is included in the scientometric base SCOPUS*

<https://ieeexplore.ieee.org/abstract/document/9580984>

8. Zashcholkin K., Drozd O., Ivanova O., Bykovyy P. Formation of the Interval Stego Key for the Digital Watermark Used in Integrity Monitoring of FPGA-based Systems. *CEUR-WS*. 2020. Vol. 2623. P. 267 – 276. *Scientific periodical foreign issue, Germany, ISSN 1613-0073. The publication is included in the scientometric bases SCOPUS and Web of Science Core Collection*

<https://ceur-ws.org/Vol-2623/paper23.pdf>

9. Zashcholkin K., Drozd O., Shaporin R., Ivanova O., Drozd M. Co-Embedding Additional Security Data and Obfuscating Low-Level FPGA Program Code. *IEEE East-West Design and Test Symposium (EWDTS)*. 2020. P. 115 – 119. DOI: <https://doi.org/10.1109/EWDTS50664.2020.9225111>. *Scientific periodical foreign issue, USA, ISSN: 2373-826X. The publication is included in the scientometric base SCOPUS*

<https://ieeexplore.ieee.org/document/9225111>

10. Patent for invention No. 122276 Ukraine, IPC G06F 11/263 (2006.01), G06F 7/544 (2006.01). Programmable device for calculating a logical function of N variables / K.V. Zashcholkin, O.V. Drozd, R.O. Shaporin, O.M. Ivanova, Y. V. Drozd; applicant Odessa National Polytechnic University. – No. a201811671; declared on 27.11.2018; published on 12.10.2020; Bull. No. 19/2020.

<https://sis.nipo.gov.ua/uk/search/detail/1458192>

***Publications of approbation type***

11. Antoschuk S.H., Ivanova O.M., Zashcholkin K.V. Steganographic embedding of additional data into the program code of FPGA. *Prospective directions of modern electronics, information and computer systems, MEICS-2023: materials of the VIII All-Ukrainian scientific and practical conference*. Dnipro, 2023.

[https://www.dnu.dp.ua/docs/ndc/2023/materiali%20konf/25\\_MEICS-2023.pdf](https://www.dnu.dp.ua/docs/ndc/2023/materiali%20konf/25_MEICS-2023.pdf)

12. Ivanova O.M., Drozd O.V., Zashcholkin K.V. Features of steganographic non-equivalent embedding of digital watermarks into FPGA program code. Features of steganographic non-equivalent embedding of digital watermarks into FPGA program code. Informatics, Control and Artificial Intelligence, ICAI-2021: theses of the VIII International Scientific and Technical Conference. Kharkiv, 2021.

[https://web.kpi.kharkov.ua/ai/wp-content/uploads/sites/249/2024/10/TEZY\\_YUYU\\_2021.pdf](https://web.kpi.kharkov.ua/ai/wp-content/uploads/sites/249/2024/10/TEZY_YUYU_2021.pdf)

13. Ivanova O.M., Mikhailov D.O., Zashcholkin K.V. An approach to 3D steganographic data embedding and its software implementation. *Modern Information Technologies, MIT-2021: Proceedings of the XI International Scientific Conference*. Odesa, 2021. P. 36 – 37.

***Publications that additionally demonstrate the results of the thesis***

14. Drozd O., Maevsky D., Maevskaya O., Martynyuk O., Parkhomenko A., Gladkova O., Drozd M., Ivanova O., Surkov S., Zashcholkin K. Internet of Things for Smart Building and City. Ministry of Education and Science of Ukraine, Odessa National Polytechnic University, Zaporizhzhia National Technical University, 2019. 156 p.

[https://aliot.eu.org/wp-content/uploads/2020/01/ALIOT\\_ITM2\\_IoT-for-Smart-Build-and-City\\_web.pdf](https://aliot.eu.org/wp-content/uploads/2020/01/ALIOT_ITM2_IoT-for-Smart-Build-and-City_web.pdf)