ЗМІСТ

РОЗДІЛ 1. ОСНОВНІ ПОЛОЖЕННЯ БАГАТОРІВНЕВОЇ ПЛАТФОРМИ КІБЕРФІЗИЧНИХ СИСТЕМ, НАПРЯМИ ТА ОРГАНІЗАЦІЯ НАУКОВИХ ДОСЛІДЖЕНЬ 13
1.1. Основні положення кіберфізичних систем 13
1.2. Застосування кіберфізичних систем 17
1.3. Напрацювання попередніх років у межах концепції КФС 21
1.4. Актуальність створення багаторівневої платформи кіберфізичних систем 24
1.5. Об'єкт, предмет та мета проведення досліджень кіберфізичних систем 24
1.6. Постановка завдання дослідження 25
1.7. Основні ідеї дослідження та шляхи їх втілення 26
1.8. Основні гіпотези, покладені в основу наукового дослідження 27
1.9. Особливості кіберфізичних систем 28
1.10. Проблеми створення кіберфізичних систем та підходи до їх вирішення 29
1.11. Архітектура кіберфізичних систем 31
1.11.1. Багаторівнева платформа для створення прикладних кіберфізичних систем 31
1.11.2. Складові багаторівневої платформи для створення прикладних кіберфізичних систем та напрями наукових досліджень в її межах 33
1.11.2.1. Фізичний світ 33
1.11.2.2. Засоби взаємодії з фізичним світом 33
1.11.2.3. Засоби збору та доставки даних 36
1.11.2.4. Засоби опрацювання даних 37
1.11.2.5. Засоби прийняття рішень 39
1.11.2.6. Засоби персонального сервісу 40
1.11.2.7. Структурна організація багаторівневої платформи кіберфізичних систем 42
1.11.2.8. Основні принципи організації міжрівневої та внутрішньорівневої взаємодії в кіберфізичних системах 44
1.11.2.9. Організація захищеної інформаційної взаємодії рівнів кіберфізичних систем 45
1.12. Переваги використання багаторівневої платформи кіберфізичних системах 46
1.13. Наукові напрями створення багаторівневої платформи кіберфізичних систем 48
1.13.1. Кластери наукових досліджень 48
1.13.2. Кластер архітектурного рівня 48
1.13.3. Кластер інтелектуальних засобів взаємодії з фізичним світом та збору і доставки даних 49
1.13.4. Кластер інтелектуальних засобів опрацювання даних

кіберфізичних систем 50
1.13.5. Кластер проблем імплементації кіберфізичних систем 51
Висновки до розділу 1 53
Література 55
РОЗДІЛ 2. ПРИНЦИПИ ПОБУДОВИ ТА ПРОЕКТУВАННЯ ОПЕРАЦІЙНИХ ВУЗЛІВ ДЛЯ ПОЛІВ ГАЛУА, ЩО ВИКОРИСТОВУЮТЬСЯ В ЗАДАЧАХ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ 58
2.1. Кіберфізичні системи 59
2.2. Алгоритмічні основи проектування комп'ютерних засобів КФС 59
2.3. Засоби криптографічного захисту інформації кіберфізичних систем 59
2.4. Методи забезпечення захисту інформації кіберфізичних систем 60
2.5. Криптографія еліптичних кривих 61
2.6. Засоби забезпечення захищеності КФС 62
2.7. Принципи використання електронного цифрового підпису 63
2.8. Стійкість засобів криптографічного захисту інформації 64
2.9. Стандарти, що використовують еліптичні криві 64
2.10. Поля Галуа як математична основа електронних цифрових підписів 67
2.11. Складність пристроїв опрацювання елементів полів Галуа 68
2.12. Вплив технологій квантових обчислень на криптографічний захист інформації 69
2.13. Криптографія ізогіней суперсингулярних еліптичних кривих 71
2.14. Особливості архітектури засобів КЗІ 71
2.15. Використання вузлів опрацювання елементів полів Галуа для роботи з цифровими підписами 74
2.16. ПЛІС, ядра та генератори ядер як елементна база спеціалізованих комп'ютерних систем 75
2.17. Вузли та структурні алгоритми множення в полях Галуа GF(2p) 76
2.18. Спецпроцесори для реалізації алгоритмів на основі еліптичних кривих 76
2.19. Математичні пакети для проведення обчислень у полях Галуа. 76
2.20. Маскування роботи цифрових пристроїв 79
2.21. Основи проектування засобів КЗІ КФС на базі операційних вузлів для полів Галуа, що використовуються при криптографічному захисті інформації на основі еліптичних кривих 80
2.22. Основні архітектурні принципи побудови операційних вузлів для полів Галуа, що використовуються при криптографічному захисті інформації на основі еліптичних кривих 81
2.23. Реалізація операційних вузлів для полів Галуа, що використовуються при криптографічному захисті інформації на основі еліптичних кривих 81
2.24. Підходи до проектування операційних вузлів для полів Галуа, що використовуються при криптографічному захисті інформації на основі

еліптичних кривих 82
2.25. Деталізація вимог щодо захисту роботи засобів КЗІ 82
2.26. Деталізація вимоги щодо роботи із електронним цифровим підписом 82
2.27. Особливості реалізації засобів КЗІ на ПЛІС 83
2.28. Вибір поля Галуа на основі оцінювання ємнісної складності представлення елементів полів Галуа 83
2.29. Вбудований контроль вузлів, що опрацьовують елементи розширених полів Галуа 83
2.30. Часова складність помножувачів для полів Галуа 87
2.31. Структурна складність помножувачів елементів полів Галуа в нормальному та поліноміальному базисах 94
2.32. Програмно-часова складність помножувачів для поліноміального базису 103
2.33. Апаратна реалізація алгоритмів роботи із цифровими підписами 107
2.34. Спецпроцесор для опрацювання елементів розширених полів Галуа 108
2.35. Маскування при знаходженні оберненого елемента в двійкових полях Галуа для поліноміального базису. Інвертори. 110
2.36. Генератор ядер для створення вузлів GF-процесора. 111
2.37. Інвертори на основі біт-паралельних помножувачів 112
2.38. Інвертори на основі паралельних помножувачів 116
2.39. Маскування операційних вузлів для полів Галуа, що використовуються при криптографічному захисті інформації на основі еліптичних кривих 120
Висновки до розділу 2 121
Література 122
РОЗДІЛ 3. АВТОМАТИЧНИЙ СИНТЕЗ КОМП'ЮТЕРНИХ ПРИСТРОЇВ В РЕКОНФІГУРОВНИХ АПАРАТНИХ ПЛАТФОРМАХ ВУЗЛІВ ІНТЕЛЕКТУАЛЬНИХ СЕНСОРІВ І АКТЮАТОРІВ КІБЕРФІЗИЧНИХ СИСТЕМ 132
3.1. Вигоди від застосування ПЛІС в компонентах КФС 132
3.2. Застосування і будова інтелектуальних сенсорів та актюаторів на базі ПЛІС 135
3.2.1. Інтелектуальний сенсор для виявлення і класифікації порушень якості енергоживлення 135
3.2.2. Інтелектуальний сенсор для отримання динамічних та коливних параметрів у промислових роботизованих системах 136
3.2.3. Інтелектуальний сенсор для оцінювання транспірації рослин у реальному часі 138
3.3. Проблеми ефективного застосування вузлів інтелектуальних сенсорів і актюаторів на базі ПЛІС в КФС 139
3.4. Огляд базових підходів до вирішення проблем застосування в КФС вузлів інтелектуальних сенсорів і актюаторів на базі ПЛІС 140

3.4.1. Метод самоконфігурування комп'ютерної системи з реконфігуровною логікою
3.4.2. Модель надання програмних засобів як сервісу через комп'ютерну мережу 140
3.4.3. Технологія Інтернету речей 142
3.5. Метод автоматичного синтезу комп'ютерних пристроїв в реконфігуровних апаратних платформах вузлів інтелектуальних сенсорів і актюаторів КФС 143
3.6. Протокол обміну інформацією між системою генерування конфігурацій і вузлом інтелектуальних сенсорів і актюаторів КФС для автоматичного синтезу комп'ютерних пристроїв в його РАП 145
3.6.1. Повідомлення і середовище їх передачі 148
3.6.2. Скінчений автомат сервера 148
3.6.3. Скінчений автомат клієнта 149
3.6.4. Приклад комунікації клієнта із сервером 151
3.7. Формат пакета даних для обміну інформацією в КФС між системою генерування конфігурацій і вузлом інтелектуальних сенсорів і актюаторів 152
3.8. Імплементація програмних засобів реалізації протоколу обміну інформацією між системою генерування конфігурацій і вузлами інтелектуальних сенсорів і актюаторів КФС 154
3.8.1. Визначення вимог до програмних засобів реалізації протоколу 155
3.8.2. Реалізація деяких нефункціональних вимог, що висувають до ПЗ на етапі розробки 155
3.8.3. Моделювання базових складових процесу взаємодії 157
3.8.4. Верифікація програмних засобів реалізації протоколу 158
Висновки до розділу 3 160
Література 162
РОЗДІЛ 4. ВЕНДИНГОВІ КІБЕРФІЗИЧНІ СИСТЕМИ 163
4.1 Особливості та життєвий цикл ВКФС 167
4.2 Організація вендингової кіберфізичної системи. 171
4.3 0-й рівень. Фізичний світ 174
4.4 1-й рівень. Засоби взаємодії з фізичним світом (вендингові автомати) 175
4.4.1 Узагальнена структура та функції вендингових автоматів 177
4.4.2 Алгоритми роботи вендингових автоматів 180
4.4.3 Інтерфейси та протоколи взаємодії комп'ютерної системи керування з периферійними пристроями вендингового автомату 182
4.4.4 Методи та пристрої оплати за товар чи послугу 183
4.4.4.1 Пристрої готівкової оплати 189
4.4.4.2 Пристрої безготівкової оплати 190
4.4.4.2.1 Пристрої для оплати банківськими картками 192
4.4.4.2.2 Пристрої для реалізації системи лояльності 192
4.4.4.3 Системи лояльності клієнтів 193
194

4.5 2-й рівень. Засоби збору та доставки інформації 201
4.6 3-й рівень. Засоби опрацювання інформації 205
4.6.1 Процес взаємодії між компонентами ВКФС на 3-му рівні 205
4.6.2 Структура апаратного забезпечення СПАК 210
4.6.3 Методи оновлення програмного забезпечення вендингових автоматів 211
4.7 4-й рівень. Засоби прийняття рішень 212
4.7.1 Профіль вендингових автоматів 214
4.7.2 Використання мереж Кохонена в ВКФС 214
4.8 5-й рівень. Засоби персонального сервісу 219
4.9 Система автоматизованого тестування ВКФС 221
4.9.1 Формат тестів (скриптів) 225
4.10 Приклад реалізації ВКФС для парковок закритого типу 226
4.10.1 Алгоритм робрти в'їзної стійки 229
4.10.2 Методика визначення конфігурації та параметрів обладнання КФСУП 230
4.10.3 Перевірка працездатності системи 233
Висновки до розділу 4 234
Література 235