Фам Зуй Тхай. Математическое обеспечение системы идентификации личности по отпечаткам пальцев с учётом особенностей их использования во вьетнаме: диссертация ... кандидата технических наук: 05.13.11 / Фам Зуй Тхай;[Место защиты: Московский государственный университет инфомационных технологий, радиотехники и электроники].- Москва, 2015.- 154 с.

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО

ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

Московский государственный университет инфомационных технологий,

радиотехники и электроники

На правах рукописи

Фам Зуй Тхай

МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СИСТЕМЫ

ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ПО ОТПЕЧАТКАМ ПАЛЬЦЕВ С

УЧЁТОМ ОСОБЕННОСТЕЙ ИХ ИСПОЛЬЗОВАНИЯ ВО ВЬЕТНАМЕ

Специальность:

05.13.11 - Математическое и

программное обеспечение

вычислительных машин, комплексов и

компьютерных сетей

Диссертация на соискание ученой степени кандидата технических наук

Научный руководитель:

д.т.н., профессор В.М.Ткаченко

МОСКВА 2015

ОГЛАВЛЕНИЕ

1 ГЛАВА 1. ОБЗОР ТЕХНОЛОГИЙ СМАРТ-КАРТЫ И БИОМЕТРИИ С

УЧЁТОМ ОСОБЕННОСТЕЙ ВО ВЬЕТНАМЕ. . 12

1.1 Смарт-карты – история и перспективы. . 12

1.2 Классификация смарт-карт 13

1.3 Фазы жинзненого цикла смарт-карт 15

1.4 Стандарты и спецификации для смарт-карт 19

1.4.1 Стандарты ISO 7816 20

1.4.2 Стандарты GSM 20

1.4.3 Спецификация ЕМѴ 21

1.4.4 Спецификации Open Platform 21

1.4.5 Интегрированная среда OpenCard Framework 22

1.4.6 Спецификации РС/SС 22

1.5 Взаймодействие со смарт-картами 23

1.5.1 Устройства считывания карт и хостприложения 23

1.5.2 Модель взаимодействия со смарт-картами 23

1.6 Анализ моделей угроз безопасности смарт-карт. . 24

1.6.1 Атаки терминала против владельца карты или владельца информации. . 25

1.6.2 Атаки владельца карты против терминала. . 25

1.6.3 Атаки владельца карты против владельца информации. . 26

1.6.4 Атаки владельца карты против поставщика услуг. . 26

1.6.5 Атаки владельцем карты против производителя программного обеспечения. 27

1.7 Биометрические системы и смарт-карты 27

1.8 Использование смарт-карт в системах безопасности во Вьетнаме 29

1.9 Выводы к главе 1 32

2 ГЛАВА 2 МЕТОДЫ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ И

МОДЕЛЬ СИСТЕМЫ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ НА ОСНОВЕ

МНОГОФАКТОРНОЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ. ... 33

2.1 Обзор технологий автоматической идентификации 33

2.1.1 Штрих-кодовая идентификация 33

2.1.2 Биометрическая идентификация; 34

2.1.3 Радиочастотная идентификация 35

2.1.4 Карточные технологии идентификации 36

2.2 Теоретические основы биометрических технологий 37

2.3 Обзор методов биометрической идентификации 38

2.3.1 Статические методы биометрической идентификации 38

2.3.1 Динамические методы биометрической идентификации 46

2.4 Общие принципы и методы построения систем биометрической

идентификации 49

2.4.1 Биометрическая идентификация и верификация 49

2.4.2 Биометрическая регистрация 53

2.4.3 Особенности аутентификации биометрической системы 55

2

2.4.4 Качество работы системы и вопросы разработки 55

2.4.5 Принципы работы систем биометрической идентификации личности 58

2.5 Математическое и программное обеспечение системы идентификации

личности на основе многофакторной биометрической аутентификации 59

2.5.1 Описание модели cистемы идентификации личности на основе многофакторной биометрической аутентификации 60

2.5.2 Разработка модели cистемы идентификации личности на основе многофакторной биометрической аутентификации 62

2.5.3 Программная архитехтура системы идентификации личности на основе многофакторной биометрической аутентификаци 66

2.6 Выводы к главе 2 68

3 ГЛАВА 3 МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СИСТЕМЫ

ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ПО ОТПЕЧАТКАМ ПАЛЬЦЕВ. . 69

3.1 Биометрия по отпечаткам пальцев 69

3.1.1 Приемлемость биометрии по отпечаткам пальцев 69

3.1.2 Основные элементы биометрической системы доступа по отпечаткам пальцев 70

3.1.3 Концепции биометрических систем доступа по отпечаткам пальцев 71

3.2 Анализ методов распознания отпечатков пальца 71

3.2.1 Классификация отпечатков пальцев 71

3.2.2 Принцип распознавания отпечатка пальца 73

3.2.3 Классы алгоритмов сравнения отпечатков пальца 78

3.2.4 Реализации алгоритмов сравнения отпечатков пальца 81

3.3 Триангуляция Делоне 83

3.3.1 Определения 83

3.3.2 Теорема построения триангуляции Делоне 86

3.3.3 Проверка условия Делоне 88

3.4 Разработка алгоритма распознавания отпечатков с целью использования

на смарт-карте 91

3.4.1 Анализ отпечатков пальцев с использованием триангуляции Делоне 91

3.4.2 Подход к разработке алгоритмы распознавания отпечатков пальцев 95

3.4.3 Распознавание отпечатков пальцев с применением нечеткой триангуляции Делоне 96

3.4.4 Cопоставление отпечатков пальцев с использованием нечёткой триангуляции Делоне 100

3.5 Выводы к главе 3 102

4 РАЗРАБОТКА МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ

БЕЗОПАСНОСТИ БИОМЕТРИЧЕСКОЙ СИСТЕМЫ

ИДЕНТИФИКЦИИ С ИСПОЛЬЗОВАНИЕМ СМАРТ-КАРТЫ 104

4.1 Принципы защиты информации, записанной на смарт-картах, рекомендованные государственным комитетом по информационной безопасности Вьетнама 104

4.2 Криптография 106

4.2.1 Шифрование и расшифровка 107

4.2.2 Дайджест сообщения 111

3

4.2.3 Цифровая подпись 112

4.3 Метод обеспечения информационной бесзопасности систем электронной

идентификации. . 114

4.3.1 Аутентификация с использованием симметричного шифрования 115

4.3.2 Аутентификация с использованием хэш-функций 117

4.3.3 Аутентификация, основанная на асимметричных алгоритмах 118

4.3.4 Биометрические аутентификационные протоколы 121

4.4 Методы обеспечения безопасности смарт-карты 125

4.4.1 Защита от физических методов атаки и подделки: 126

4.4.2 Аппаратно-программные методы защиты смарт-карт 126

4.4.3 Криптографические методы защиты смарт-карты: 129

4.5 Разработка метода биометрической аутентификации с использованием

смарт-карты 131

4.5.1 Требования к смарт-картам 131

4.5.2 Использование биометрии 132

4.5.3 Использование криптографии 133

4.5.4 Безопасный протокол 134

4.5.5 Процедуры системы идентификации личности с использованием смарт-карты. 135

4.6 Выводы к главе 4 138

ЗАКЛЮЧЕНИЕ 140

ЛИТЕРАТУРА 142

ПРИЛОЖЕНИЕ 1 148

Алгоритм распознавания и сравнения по отпечаткам пальцев 148

ПРИЛОЖЕНИЕ 2 149

Документы об использовании результатов диссертационной работы 149

Протокол о внедрении Центра информационной технологии – Государственный

Комитет по информационной безопасности Вьетнама 149

Протокол о внедрении компания ОАО «TP ТОРГОВЛИ И ТЕХНОЛОГИИ» 151

Акт о внедрении компании ООО «НАМ ТАМ ГРУПП» 153

Акт о внедрении результатов диссертационной работы в учебном процессе МГТУ

МИРЭА 154

ЗАКЛЮЧЕНИЕ

· Проведен анализ состояния исследований особенностей смарт-

карт в настоящее времея, их прицпипы классификации, стандарты и

спецификации, угрозы бесзопасности. Рассмотрено взаймодействие между

биометрической системой и смарт-картой с целью выработки требования к

созданию биометрической системы идентификации личности с

использованием смарт-карты в СРВ с учётом существующей экономической

ситуации страны и уровнем ее технологического развития.

· Определены требования к биометрической системе

идентификации с использованием смарт-карты с учётом особенностей их

использования во Вьетнаме[70].

· Разработана модель и программная архитектура системы

идентификации личности на основе многофакторной биометрической

аутентификации.

· Разработан алгоритм распознавания и сравнения отпечатков

пальцев с использованием нечёткой триангуляции Делоне[69-70],

применения разработанных алгоритмов в системе идентификации во

Вьетнамских государственных органах, компаниях доказал эффективность и

надёжность при идентификации личности.

Результаты работы использованы Центром информационной технологии – Государственного Комитета по информационной Безопасности Вьетнама (Vietnam Goverment Information Security Committee) при создании системы идентификации личности c использованием смарт-карты в государственных органах. Спецификации алгоритма распознавания и сравнения отпечаткам пальцев с использованием смарт-карты применены компанией ООО «НАМ ТАМ ГРУПП» и Вьетнамской ОАО компанией «TP ТОРГОВЛИ И ТЕХНОЛОГИИ» при разработке системы контроля доступа и рабочего времени.

140

Материалы диссертационной работы были использованы в учебном процессе МИРЭА при изучении дисциплин «Структуры и алгоритмы обработки данных», «Защита информации», «Системы искусственного интеллекта» и «Проектирование информационных систем».