МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт Факультет приборостроения, информационных технологий и электроники	Кафедра «Информационная безопасность систем и технологий»
Специальность 10.05.02 –	Информационная безопасность телекоммуникационных систем
Специализация -	Разработка защищенных телекоммуникационных систем

ДИПЛОМНАЯ РАБОТА

на тему

СПОСОБЫ ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ В БИОМЕТРИЧЕСКИХ СИСТЕМАХ

Студент _____ Павлов Максим Александрович

Руководитель _____ Секретов М.В.

Нормоконтролёр _____ Фатеев А.Г.

Рецензент научный сотрудник лаборатории биометрических и нейросетевых технологий АО "ПНИЭИ" Калашников Д.М.

Работа допущена к защите (протокол заседания кафедры от _____ № _____)

Заведующий кафедрой _____ С.Л. Зефиров

Работа защищена с отметкой _____(протокол заседания ГЭК от _____ № ____)

Секретарь ГЭК _____ А.Г. Фатеев

Пенза 2016

РЕФЕРАТ

Отчет 89 с., 34 рис., 3 табл., 26 источников, 3 прил.

БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ, НЕЧЕТКИЙ ЭКСТРАКТОР, НЕЙРОСЕТЕВОЙ ПРЕОБРАЗОВАТЕЛЬ БИОМЕТРИЯ-КОД, БИОМЕТРИЧЕСКИЙ ОБРАЗ, ОТПЕЧАТОК ПАЛЬЦА, КОРРЕКТИРУЮЩИЙ КОД.

Объектом исследования являются методы обезличивания данных, нечеткие экстракторы и нейросетевые преобразователи, преобразующие биометрические данные человека в код доступа для его использования в средствах аутентификации.

Цель работы – разработка способов обезличивания персональных данных в биометрических системах с использованием нейросетевых преобразователей биометрия-код и нечетких экстракторов.

В ходе дипломного проектирования рассмотрены существующие методы обезличивания персональных данных, отмечены их недостатки, заключающиеся в необходимости использования при обработки операторами сведений, идентифицирующих человека и удостоверяющих его личность. Для информационных систем, в которых обрабатываются биометрические данные, требуется разработка способов обезличивания, учитывающих особенности таких систем.

В результате дипломного проектирования разработаны способы и алгоритмы обезличивания персональных данных в биометрических системах, в которых выполняется аутентификация личности. Применение разработанных способов позволяет при обработке ограничить доступ операторам к информации, идентифицирующей человека. Проведена статистическая оценка работы биометрических систем с использованием моделей преобразователя на основе искусственной нейронной сети и преобразователя на основе помехоустойчивого кода. Выполнено сравнение вероятностных характеристик моделей, с применением баз данных "Свой" и "Чужой", полученных в программной среде сбора отпечатков пальцев.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УДК 004.056

Политехнический институт

УТВЕРЖДАЮ

Факультет приборостроения, информационных технологий и электроники

Зав. кафедрой ИБСТ
к.т.н., доцент С.Л. Зефиров

Выпускающая кафедра:
Информационная безопасность систем и технологий

«___» _____ 2016 г.

Учебная группа 11ПТ1

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

студента группы 11ПТ1 Павлова Максима Александровича

Специальность 10.05.02 – Информационная безопасность телекоммуникационных систем

Тема дипломной работы:

Способы обезличивания персональных данных в биометрических системах

Руководитель ВКР
к.т.н., научный сотрудник, ЛБНТ АО ПНИЭИ М.В.Секретов

Нормоконтролер
к.т.н., доцент кафедры ИБСТ А.Г. Фатеев

1 Цели и задачи ВКР

Цель работы – разработка способов обезличивания персональных данных в биометрических системах с использованием нейросетевых преобразователей биометрия-код и нечетких экстракторов, включающая:

– анализ возможностей биометрических систем с нейросетевыми преобразователями;

– анализ возможностей биометрических систем с нечеткими экстракторами;

– разработку алгоритмов обезличивания персональных данных в биометрических системах для двух технологий преобразования биометрических данных;

– построение базы данных «Свой» 100 образов по 20 примеров;
построение базы данных «Чужой» 100 образов по 1 примеру;
статистическую оценку работы биометрических систем.

2 Тактико – технические требования к выполнению ВКР

Технические требования:

– должен быть представлен способ обезличивания персональных данных с использованием нейросетевого преобразователя биометрия-код;

– должен быть представлен способ обезличивания персональных данных с использованием нечеткого экстрактора;

– при обучении нейросетевого преобразователя должна быть использована обучающая выборка, содержащая не менее 10 примеров биометрического образа;

– должны быть построены базы данных «Свой» и «Чужой» для оценки вероятности ошибок первого и второго рода;

– должна быть написана программа для статистической оценки работы биометрических систем.

В ВКР должны быть рассмотрены следующие вопросы:

- анализ отечественных и зарубежных технологий преобразования биометрических данных;

– достоинства и недостатки технологий преобразования биометрических данных;
– анализ методов и алгоритмов обезличивания персональных данных;
– достоинства и недостатки технологий преобразования биометрических данных;
– описание разрабатываемых способов.

3 Требования к разрабатываемой документации

Отчет по ВКР выполняется в соответствии с требованиями ГОСТ 7.32.

Перечень и содержание графической части ВКР:

– программная среда сбора биометрических данных – 1л., ф. А1 (плакат);

– структура нейросетевых преобразователей – 1л., ф. А1 (плакат);

– структура нечетких экстракторов – 1л., ф. А1 (плакат);

– алгоритм обезличивания персональных данных с использованием нейросетевых преобразователей – 1л., ф. А1 (плакат);

– алгоритм обезличивания персональных данных с использованием нечетких экстракторов – 1л., ф. А1 (плакат);

– статистическая оценка работы биометрических систем– 1л., ф. А1 (плакат).

Электронная копия отчета и графической части ВКР должна быть представлена на магнитном или оптическом носителе.

4 Сроки выполнения ВКР

Тема утверждена приказом ректора ПГУ № ____ от «___» _____ 2016 г.

Дата выдачи задания «30» августа 2016 г.

Время дипломного проектирования с 10 октября 2016 г. по 15 января 2017 г.

Задание к исполнению принял «30» августа 2016 г.

Исполнитель ВКР _____Павлов М.А.

СОДЕРЖАНИЕ

Введение 12

1 Анализ биометрических систем и способов их защиты 15

1.1 Биометрические характеристики человека 15

1.2 Тайные и открытые биометрические образы 17

1.3 Характеристика классических биометрических систем 19

1.4 Способы защищенной биометрической аутентификации 23

1.5 Нечеткие экстракторы 26

1.6 Нейросетевые преобразователи биометрия-код 29

1.7 Выводы по первому разделу 31

2 Разработка способов обезличивания персональных данных в биометрических системах 33

2.1 Методы обезличивания персональных данных 33

2.1.1 Метод введения идентификаторов 33

2.1.2 Метод изменения состава или семантики 34

2.1.3 Метод декомпозиции 36

2.1.4 Метод перемешивания 37

2.2 Вычисление биометрических параметров отпечатка пальца 38

2.2.1 Двоичные биометрические параметры 38

2.2.2 Непрерывные биометрические параметры 40

2.3 Способ обезличивания персональных данных с использованием нейросетевого преобразователя биометрия-код 46

2.4 Способ обезличивания персональных данных с использованием нечеткого экстрактора 48

2.5 Выводы по второму разделу 52

3 Моделирование способов обезличивания персональных данных в биометрических системах 54

3.1 Программная среда сбора отпечатков пальцев 54

3.2 Построение баз данных «Свой» и «Чужой» 63

3.3 Моделирование нейросетевого преобразователя биометрия-код и нечеткого экстрактора 64

3.4 Статистическая оценка принимаемых решений биометрической системой 70

3.5 Выводы по третьему разделу 73

Заключение……..……...75

Список использованных источников 77

Приложение А Текст программы для статистической оценки нейросетевых преобразователей и нечетких экстракторов 80

Приложение Б Результаты моделирования нечеткого экстрактора и нейросетевого преобразователя 84

Приложение В Результаты прохождения ВКР в системе "Антиплагиат"…… ……...88

ОПРЕДЕЛЕНИЯ

В настоящей работе применяют следующие термины с соответствующими определениями:

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение личности субъекта. [24]

Биометрическая аутентификация – аутентификация человека, осуществляемая путем предъявления им своего биометрического образа. [11]

Биометрические данные – сведения, которые характеризуют физиологические, поведенческие и биологические особенности человека. [11]

Биометрический контейнер – набор данных, позволяющий получить из биометрического образа субъекта доступа информацию аутентификации в виде кода доступа. [16]

Биометрические параметры – параметры, полученные после предварительной обработки биометрических данных. [11]

Биометрический образ – образ человека, полученный с выходов первичных измерительных преобразователей физических величин биометрической характеристики. [11]

Биометрический образ «Свой» – биометрический образ легального пользователя. [11]

Биометрический образ «Чужой» – биометрический образ злоумышленника, пытающегося преодолеть биометрическую защиту. [11]

Биометрический шаблон – биометрические данные, представляющие значимые биометрические характеристики человека и используемые биометрической системой для сравнения с получаемыми биометрическими образцами. [18]

Защищенный биометрический контейнер – биометрический контейнер, имеющий защиту механизмом размножения ошибок в коде доступа. [15]

Идентификация – присвоение субъекту доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов. [18]

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств. [24]

Искусственная нейронная сеть – сеть, состоящая из искусственных нейронов и имитирующая свойства биологических нейронов для решения задач в сфере искусственного интеллекта. [16]

Искусственный нейрон – упрощённая модель биологического нейрона, которая математически описывается как некоторая нелинейная функция от единственного аргумента – линейной комбинации всех входных сигналов. [16]

Нейросетевой преобразователь биометрия-код – преобразователь на основе искусственной нейронной сети, способный преобразовывать вектор нечетких, неоднозначных биометрических параметров «Свой» в четкий однозначный код доступа (ключ). Преобразователь, откликающийся случайным выходным кодом на воздействие случайного входного вектора, не принадлежащего множеству образов «Свой». [11]

Нечеткий экстрактор – преобразователь на основе корректирующих кодов, способный преобразовывать вектор нечетких, неоднозначных биометрических параметров «Свой» в четкий однозначный код доступа (ключ). [13]

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных. [23]

Обезличенные данные – это данные, хранимые в информационных системах в электронном виде, принадлежность которых конкретному

субъекту персональных данных невозможно определить без дополнительной информации. [23]

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. [24]

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). [24]

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящей работе применяют следующие обозначения и сокращения:

БЧХ – код Боуза-Чоудхури-Хоквингема

ВБП – вектор биометрических параметров

ВКР – выпускная квалификационная работа

ИНС – искусственная нейронная сеть

ИСПДн – информационная система персональных данных

НСД – несанкционированный доступ

ПДн – персональные данные

ПС – программное средство

ПЭВМ – персональная электронная вычислительная машина

ВВЕДЕНИЕ

В настоящее время перспективным средством защиты данных от несанкционированного доступа (НСД) является многофакторная аутентификация пользователей, объединяющая несколько различного рода факторов сверки: сведения, известные пользователям, объекты, имеющиеся у пользователей и уникальные биометрические характеристики самого пользователя. Средства аутентификации на основе паролей, выдаваемых авторизованным пользователям, просты в реализации и имеют низкую стоимость. Главным недостатком таких средств, при защите данных от несанкционированного доступа, является возможная потеря конфиденциальности секретов пользователей. Человеку трудно запомнить длинные пароли. Поэтому такие пароли хранят в блокноте или в незащищенном файле на компьютере. Короткие смысловые пароли легко подбираются злоумышленником. Это делает аутентификацию по паролю слабозащищенной.

Одним из видов безопасного средства аутентификации считаются персональные устройства хранения ключевой информации: пластиковые карты, смарт-карты, токены. При наличии такого устройства, пользователю нет необходимости запоминать длинные пароли. Чтобы взломать защиту злоумышленнику необходимо украсть устройство пользователя. Заметив кражу, владелец устройства может сразу же сообщить о факте хищения службе безопасности. Стоимость средств аутентификации с использованием носителей ключевой информации выше по сравнению со средствами аутентификации с использованием обычных паролей.

Средства биометрической аутентификации используют физиологические и поведенческие особенности, которыми обладает пользователь и неразрывно связаны с ним. К средствам биометрической аутентификации относятся геометрия лица, геометрия рук, рисунок отпечатка пальца, рисунок радужной оболочки глаза, рукописный почерк,

особенности голоса. Биометрические характеристики невозможно забыть, потерять, украсть, передать другому человеку. С помощью биометрии не только проверяется подлинность пользователя, но и подтверждается его личность. Система биометрической аутентификации должна гарантировать высокую надежность, чтобы подтверждать авторизованного пользователя, но отвергать злоумышленника со схожими биометрическими параметрами, а также обеспечивать конфиденциальность биометрии как персональных данных пользователей.

Поэтому надежная идентификация пользователя системой может быть гарантирована, только если одним из факторов сверки является его уникальная биометрическая характеристика. Цены на биометрические устройства стали более приемлемыми для покупателей. Таким образом, биометрические технологии достигли стадии практического использования, и их применение в средствах защиты информации вполне целесообразно.

Однако все же остаются некоторые важные вопросы применения биометрических данных в средствах защиты. Дело в том, что использование уникальных биометрических характеристик человека требует их надежной защиты от утечки, которая может привести к серьезным последствиям. Физиологические и поведенческие особенности человека позволяют несанкционированно установить его личность, организовать за ним скрытую слежку. По этой причине некоторые пользователи отказываются от хранения свои биометрические данные, например, данные рисунка отпечатка пальца в каких-либо базах данных информационных систем, опасаясь угроз, связанных с нарушения частной жизни и конфиденциальности личности.

Актуальной задачей является безопасное хранение неточно (неоднозначно) воспроизводимых биометрических данных. Именно эта проблема делает невозможным использование криптографических хеш-функций для безопасного хранения биометрической информации. С течением времени появилось два направления по решению проблемы безопасности. Одно направление, созданное и развиваемое за рубежом,

характеризуется использованием нечетких экстракторов на основе кодов с обнаружением и исправлением ошибок.

В РФ создано и активно развивается направление нейросетевого преобразования биометрических данных человека в код доступа. Разработаны отечественные стандарты высоконадежной нейросетевой биометрической аутентификации.

Одним из эффективных способов защиты персональных данных является обезличивание. Обезличивание позволяет снизить риски несанкционированного использования и причинения ущерба в случае утечки. Биометрические данные также относятся к персональной информации, которую необходимо защищать от несанкционированного использования. Однако традиционные способы обезличивания крайне неэффективны для информационных систем, обрабатывающих биометрические данные. Поэтому актуальной задачей является разработка способов обезличивания, учитывающих особенности биометрических данных и систем их использующих.

В данной дипломной работе затрагиваются описанные выше вопросы, цель которой направлена на разработку способов обезличивания персональных данных с использованием нейросетевых преобразователей и нечетких экстракторов.

В первом разделе проведен анализ биометрических систем и способов их защиты, подробно рассматриваются нечеткий экстрактор и нейросетевой преобразователь.

Второй раздел посвящен разработке способов обезличивания персональных данных в биометрических системах.

Третий раздел посвящен моделированию способов обезличивания персональных данных в биометрических системах с использованием баз биометрических образов «Свой» и «Чужой».

1 Анализ биометрических систем и способов их защиты

1.1 Биометрические характеристики человека

Все биометрические характеристики человека можно разделить на два класса: статические и динамические характеристики [1, 2]. Статические биометрические характеристики являются физиологическими особенностями, которые не изменяются в течение жизни человека. К физиологическим особенностям относятся:

– геометрия лица;

– рисунок отпечатков пальцев;

– радужная оболочка глаза;

– геометрия рук.

Физиологические особенности могут быть утрачены в результате болезни человека, при физическом (хирургическом) воздействии на его органы.

К динамическим биометрическим характеристикам относятся:

– динамика рукописного почерка;

– голос;

– сердечный ритм;

– походка.

Не существует единственной биометрической характеристики, которая подошла бы для всех нужд. Каждая биометрическая характеристика имеет свои преимущества и недостатки. Процесс получения биометрической характеристики должен быть по возможности быстрым и простым, без причинения каких-либо неудобств человеку.

Сегодня биометрические данные лиц широко используются в информационных системах для органолептической идентификации граждан. Но с развитием средств вычислительной техники биометрические данные лиц стали успешно применяться автоматическими средствами распознавания человека для установления и подтверждения его личности. В общем случае

можно выделить два класса средств биометрической идентификации человека по лицу. Первый класс средств анализирует плоские изображения лица человека (2D портреты). Двухмерный анализ плоского изображения заключается в выделении на нем характерных точек и вычислении геометрии, а именно расстояний между центрами глаз, между линией глаз и кончиком носа и т.п.

Двухмерный анализ плоского изображения лица человека позволяет получить совсем не много биометрической информации. Переход к более сложному трехмерному анализу геометрии лица человека позволяет значительно увеличить объем получаемой биометрической информации.

Особенности папиллярного рисунка отпечатка пальца широко используются в дактилоскопии, которая сегодня является неотъемлемой и важной частью криминалистики, оперативно-розыскной деятельности. Появление малогабаритных сканеров считывания папиллярного рисунка отпечатка пальца позволило успешно использовать данные биометрические характеристики для подтверждения личности человека в системах контроля и управления доступом. Стоит отметить, что возникла острая необходимость применения отпечатков пальцев паспортно-визовыми службами и миграционной политике различных государств мира.

Радужная оболочка глаза является уникальной физиологической характеристикой человека. Сканирование основано на поглощении инфракрасного излучения меланином, отвечающего за пигментацию радужной оболочки. Параметры измеряются по получаемому изображению.

В настоящее время существует два основных подхода к идентификации геометрии руки человека. Первый подход основывается на геометрических характеристиках кисти человека. Второй относится к современным подходам, поскольку помимо геометрических параметров используют еще такие характеристики руки как расположение кровеносных сосудов.

Рукописный почерк – это динамическая характеристика, которая связана с особенностью поведения человека. Измеряемыми параметрами

являются зависимости координат конца пера от времени, получаемые, как правило, с помощью графического планшета.

Определенную степень уникальность также имеют биометрические характеристики голоса человека. Установление принадлежности разных речевых фраз одному и тому же человеку, идентификация личности по голосу применяются в криминалистике. Существуют автоматические средства распознавания способные определять параметры на основе характерных для звуков речи сигналов, имеющих свою форму колебаний давления. Известно, что часть звуков речи огласованы (являются периодическими), а другая часть звуков является шипящими (не периодическими).

Сердечный ритм и походка человека не имеют высокой степени уникальности биометрических параметров, поэтому не получили применения.

Таким образом, можно выделить положительные свойства биометрических характеристик человека. Биометрию невозможно потерять, забыть, передать другому человеку, как например другие идентификаторы: пароль, PIN-код, смарт-карту, токен. Данные свойства особенно важны для обеспечения безопасности таких систем, которую требуют надежную аутентификацию пользователей.

1.2 Тайные и открытые биометрические образы

Среди биометрических характеристик человека можно выделить те характеристики, которые могут оставаться человеком в тайне или неизвестным образом, который не раскрывается другим лицам. Данные на рисунке 1.1 отражают современную практику использования открытых биометрических образов при идентификации человека.

Наиболее удобными биометрическими технологиями с точки зрения обеспечения тайны образов являются биометрические технологии анализа голоса и рукописного почерка человека. Обеспечить тайну таких биометрических образов проще всего, достаточно голосом или своим

почерком воспроизводить парольное слово (парольную фразу). Для того, чтобы обеспечить тайну статических образов, которые не изменяются по воле человека, необходимо пользоваться системой организационно-технических мероприятий, обеспечивающих обезличивание человека. Как только сторонний наблюдатель узнает имя человека найти человека и скомпрометировать данные его статического биометрического образа не сложно. Можно сделать вывод, что тайна биометрического образа на много сильнее, чем биометрические технологии.

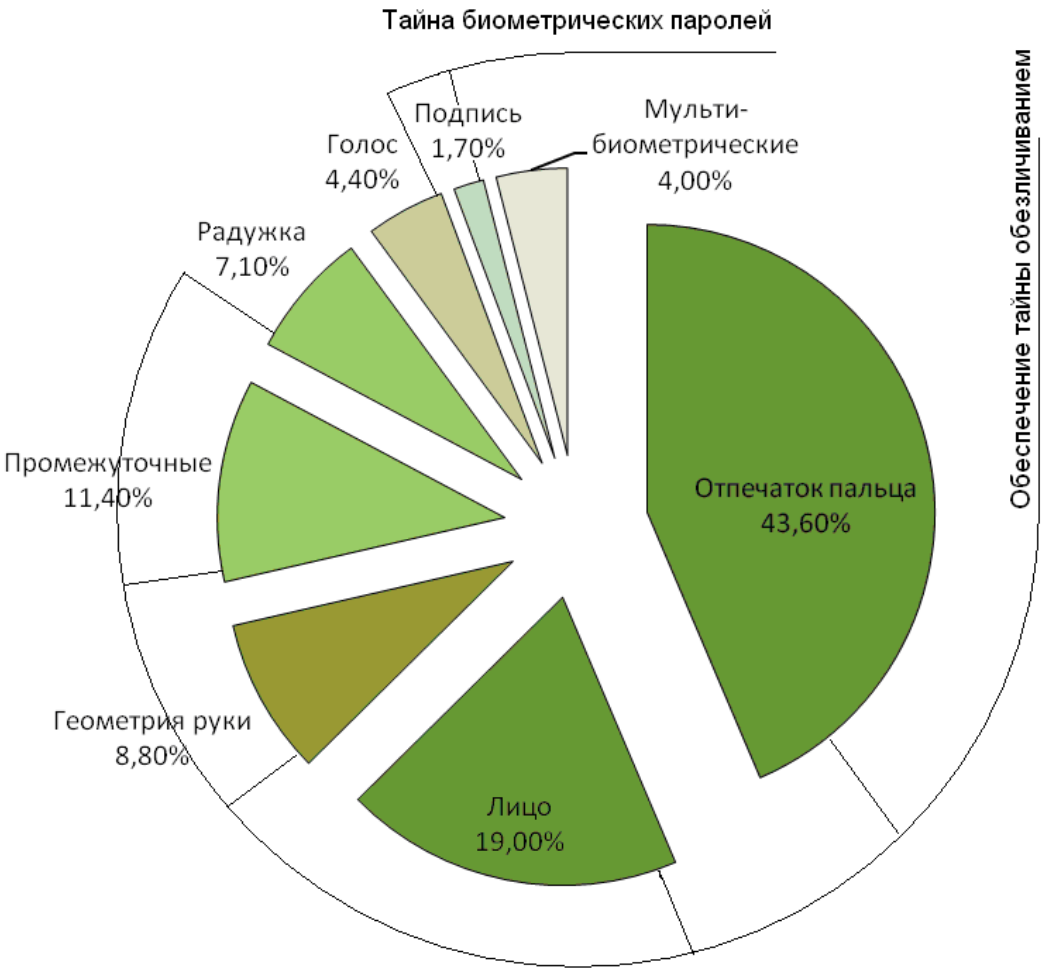

Рисунок 1.1 – Распределение востребованности биометрических технологий

На сегодняшний день наблюдается две выраженные тенденции в развитии средств защиты информации:

– массовое использование асимметричной криптографии (пары из открытого и закрытого ключа);

– усиление процедур идентификации и аутентификации с помощью биометрических технологий.

По экспертным оценкам отечественных и зарубежных исследователей безопасность использования средств асимметричной криптографии может быть усилена за счет связывания открытых и закрытых ключей с биометрией их владельца. При авторизации прав личности на управление закрытым криптографическим ключом необходимо обеспечивать сохранение в тайне закрытого биометрического образа. Открытый ключ может быть связан с открытым (общедоступным) биометрическим образом человека, например, с 3D-маской лица человека. Закрытый ключ обязательно должен быть связан с тайным (закрытым) образом человека, например, с его рукописным паролем.

1.3 Характеристика классических биометрических систем

Биометрические системы проектируются и разрабатываются для осуществления контроля доступа в охраняемые помещения, на военные объекты [3, 4, 5]. Создаются системы автоматической идентификация личности, которые используются в оперативно-розыскной деятельности правоохранительных органов [6]. В мире получают распространение системы биометрической идентификации граждан при доступе к социальным услугам, оказании медицинской помощи, голосовании, переписи населения, учете продолжительности рабочего времени, покупке товаров и т.д. [7, 8].

В качестве нормативной базы по разработке биометрических систем выступают как международные, так и отечественные стандарты [9-18].

Ветвь биометрических стандартов, ориентированных на создание биометрических систем на основе биометрических образов, сохраняемых в тайне, пока активно создается только в России. На настоящий момент разработано 8 отечественных биометрических стандартов, из которых 5 введено в действие на территории России. Организация международных усилий по стандартизации биометрических технологий отражена на рисунке 1.2.

Согласно международным стандартам простейшая биометрическая система – это автоматизированная система, которая осуществляет:

- регистрацию биометрического образа пользователя с помощью биометрического сканера;
- вычисление биометрических параметров и формирование биометрического шаблона;
- сравнение биометрических параметров с параметрами, содержащимися в биометрическом шаблоне;
- принятие решения и выдачу результата идентификации и верификации.

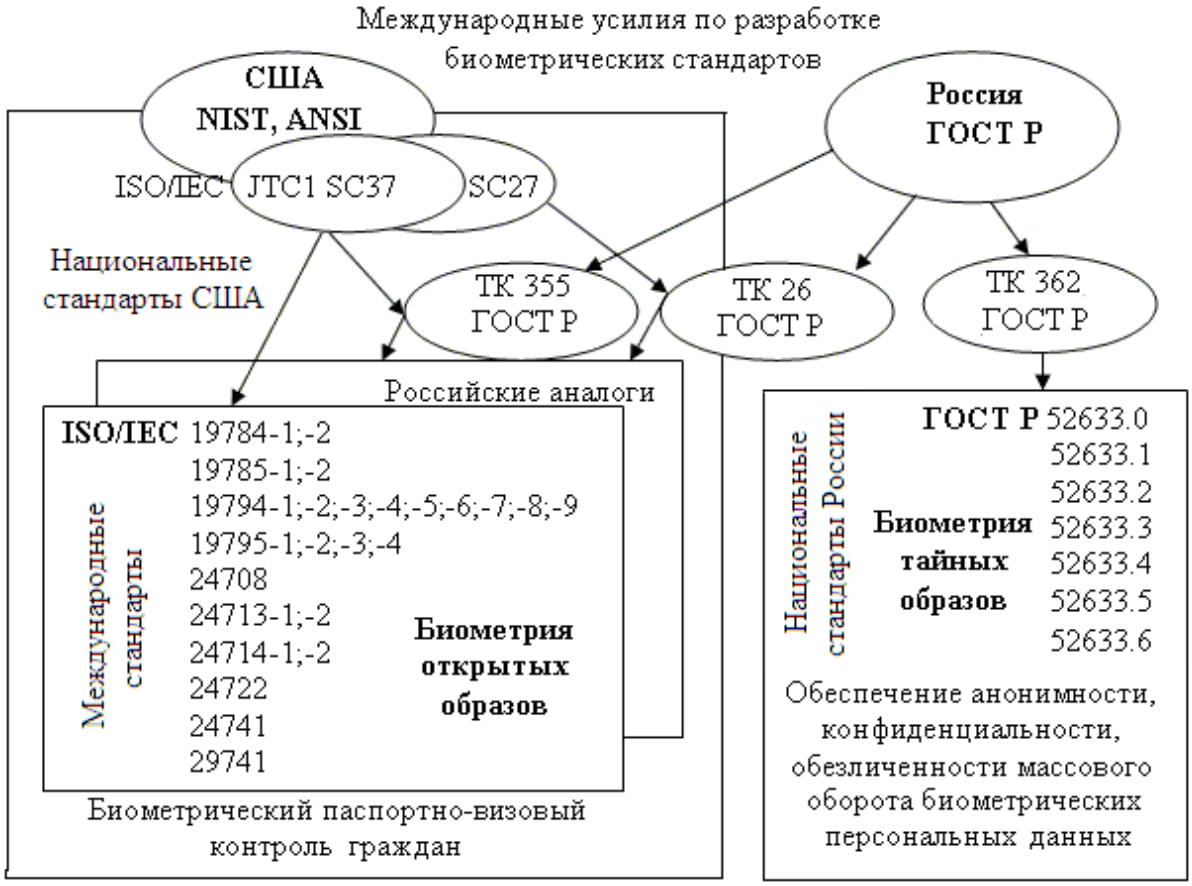

Рисунок 1.2 – Распределение международных усилий по стандартизации биометрических технологий

Биометрическая система состоит из подсистем регистрации и верификации (идентификации) пользователей. Подсистема регистрации

(обучения) осуществляет сбор биометрических данных и других сведений о пользователе (субъекте доступа), действия которого регламентируются согласно каким-либо правилам разграничения доступа. При этом данных должно быть достаточно для идентификации (присвоения идентификатора) пользователя и проверки принадлежности субъекту доступа предъявленного им идентификатора.

Типичная структура биометрической системы представлена на рисунке 1.3.

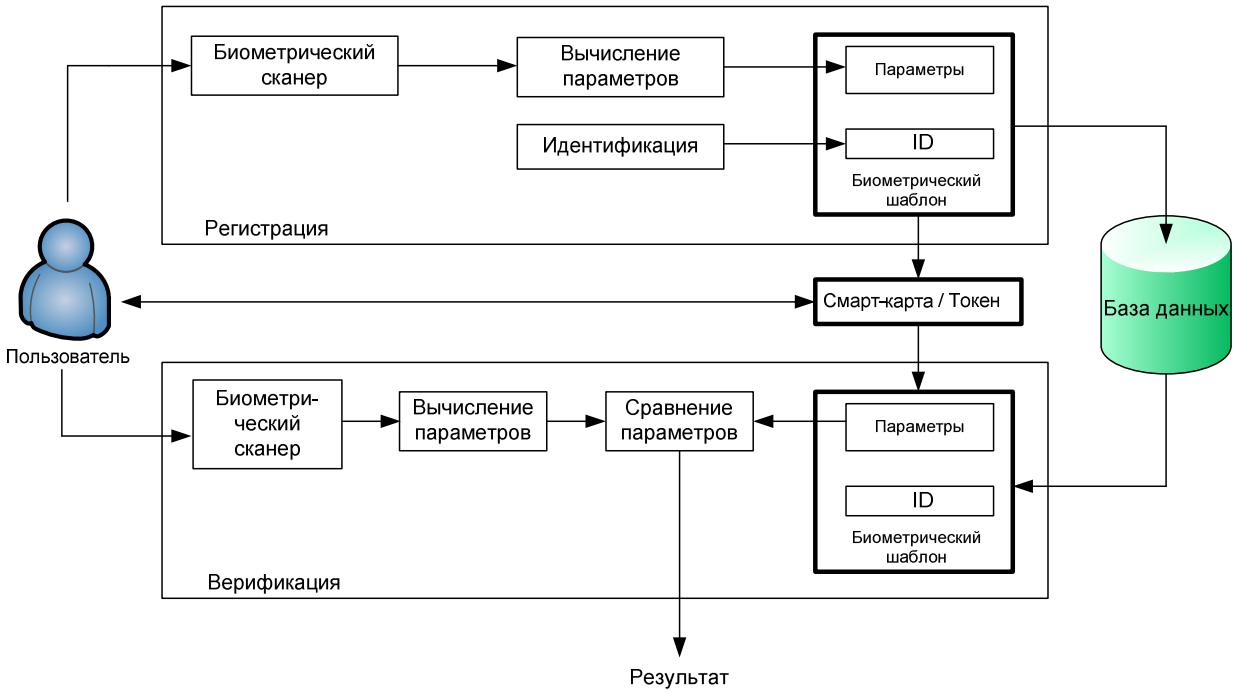

Рисунок 1.3 – Типичная структура биометрической системы

В процессе регистрации биометрический образ считывается биометрическим устройством ввода, далее выделяются значимые параметры пользователя, формируется биометрический шаблон и сохраняется в базе данных вместе с каким-либо идентификатором, который имеет пользователь либо присваивается ему в процессе регистрации. Идентификатор пользователя и биометрический шаблон могут быть размещены на смарт-карте, токене. При верификации пользователь предъявляет системе идентификатор и биометрические данные. Затем вычисляются значимые параметры пользователя, которые сравниваются с параметрами

биометрического шаблона, полученного из базы данных по предъявленному идентификатору. После чего принимается решение и дается ответ тот ли это человек, за кого он себя выдает (отображается результат «Да» / «Нет»).

Также биометрическая система может ответить на вопрос, принадлежат ли предъявляемые биометрические данные кому-либо из пользователей системы, то есть идентифицировать личность.

При сравнении биометрических параметров вычисляется некоторая мера сходства *S*, которая сравнивается с пороговым значением *T*. В том случае, если *S* больше, либо равно *T*, принимается решение о том, что предъявляемые биометрические параметры и параметры биометрического шаблона принадлежат одному человеку. Если *S* меньше *T*, принимается решение о том, что параметры принадлежат разным людям.

Основными характеристиками биометрических систем являются ошибки первого и второго рода. Когда предъявляемые биометрические параметры и параметры биометрического шаблона действительно принадлежат одному человеку, а результат их сравнения меньше порогового значения, возникает ошибка первого рода P_I. Когда предъявляемые биометрические параметры и параметры биометрического шаблона принадлежат разным людям, а результат сравнения больше порогового значения, возникает ошибка второго рода P_{II}. В таблице 1.1 приведены средние показатели P_I и P_{II} для различных биометрических систем [19].

Таблица 1.1 – Характеристики известных биометрических систем

Хар.	Лицо	Отпечаток пальца	Вены ладони	Вены пальца	Радужка	Подпись	Голос
P_I	$2{,}6 \cdot 10^{-2}$	10^{-2}	10^{-2}	10^{-2}	10^{-3}	10^{-2}	10^{-1}
P_{II}	$1{,}3 \cdot 10^{-2}$	10^{-5}	10^{-7}	10^{-5}	10^{-6}	10^{-6}	$3 \cdot 10^{-2}$

Биометрические системы, которые отвечают исключительно требованиям международных стандартов принято называть классическими биометрическими системами. Такие системы просты в реализации, но в тоже время имеют следующие значимые недостатки:

– биометрический шаблон, который хранится и обрабатывается в биометрической системе незащищен. Компрометация биометрического шаблона приводит к компрометации как тайного, так и открытого биометрического образа человека;

– однобитовый результат («Да» / «Нет») делает средства аутентификации уязвимыми к атакам, направленным на подмену результата аутентификации;

– хранение секретного криптографического ключа совместно с биометрическим шаблоном также недопустимо.

Перечисленные уязвимости классических биометрических систем могут быть устранены за счет способов защищенной биометрической аутентификации, которые основаны на следующих основных положениях. Во-первых, биометрию человека необходимо связывать с некоторым кодом доступа. Во-вторых, биометрические шаблоны не должны использоваться для принятия решения и выдачи результата идентификации и верификации.

1.4 Способы защищенной биометрической аутентификации

В 2001 году зарубежными учеными впервые были предложены способы устранения угроз нарушения конфиденциальности биометрических шаблонов в системах биометрической аутентификации и идентификации. В частности предложены способы трансформации биометрического шаблона и его преобразования с помощью полиномиальных необратимых функций.

Синтез биометрических технологий и криптографии привел к образованию биометрических криптографических систем [20]. В таких системах биометрические данные пользователя преобразуются в его личный криптографический ключ, содержатся механизмы защиты биометрического

шаблона. Данное направление получило название «биометрическое шифрование» («biometric encryption»).

Поскольку биометрические данные неточно воспроизводимы задача получения на их основе точного значения криптографического ключа является довольно сложной. В настоящее время данная технология развивается по нескольким направлениям и насчитывается несколько видов биометрических криптографических систем:

– системы с освобождением ключа (key release cryptosystem);

– системы со связыванием ключа (key binding cryptosystem);

– системы с генерацией ключа (key generation cryptosystem).

Рассмотрена каждая система более подробно, в частности принципы и способы выполняемых преобразований.

В системе с освобождением ключа хранятся и криптографический ключ и биометрический шаблон. Освобождение ключа (предоставление доступа к ключу) происходит при успешной биометрической аутентификации. В процессе аутентификации требуется доступ к биометрическому шаблону, поэтому он хранится открыто, что является недостатком. Таким образом, возможна модификация ключевой информации и данных шаблона. Достоинством систем с освобождением ключа является простота их реализации.

В системе со связыванием ключа криптографический ключ связывается с биометрическим шаблоном путем замещения его значащих данных данными извлекаемого ключа. Стойкость такой системы зависит от конфиденциальности алгоритма связывания. Тем не менее, данный вид систем может быть применим для защиты биометрических шаблонов.

В системе с генерацией ключа криптографический ключ не хранится, а извлекается непосредственно из биометрических данных пользователя, что является неоспоримым преимуществом системы. Однако реализация системы с генерацией ключа намного сложнее рассмотренных систем. Сложность заключается в необходимости создания алгоритмов вычисления

качественных биометрических параметров и генерации двоичного вектора фиксированной длины, дающего точное значение криптографического ключа легитимного пользователя при предъявлении системе одного и того же биометрического образа «Свой» и равновероятное распределение нулей и единиц при предъявлении случайных значений биометрических данных.

На сегодняшний день известны следующие подходы к преобразованию биометрических данных в криптографический ключ и применимые для разных биометрических технологий:

– нечеткие экстракторы («fuzzy extractors»);

– нечеткие хранилища («fuzzy valt»);

– биометрико-нейросетевое преобразование;

В нечетких экстракторах и нечетких хранилищах применяются коды с обнаружением и исправлением ошибок, возникающих в двоичном векторе из-за неточного воспроизведения биометрических данных [21, 22]. Качество преобразования биометрических данных в ключ во многом определяется качеством применяемых кодов, обнаруживающих и исправляющих ошибки. При вычислении криптографического ключа оба метода преобразования требуют хранения дополнительных открытых данных (открытый хелпер от англ. public helper).

По пути создания нечетких экстракторов идут в основном зарубежные исследователи. Нейросетевые преобразователи биометрия-код предложены отечественными исследователями [23]. В нейросетевых преобразователях биометрия-код используется искусственная нейронная сеть (ИНС), которая автоматически обучается на этапе регистрации пользователя формировать его личный ключ при предъявлении биометрического образа «Свой». При этом для случайных биометрических данных, примеров образов «Чужой» ИНС формирует случайную кодовую комбинацию.

Таким образом, в настоящее время существует два основных подхода к преобразованию неоднозначного биометрического образа в криптографический ключ пользователя, в дальнейшем используемый в

классических механизмах аутентификации: нечеткий экстрактор и нейросетевой преобразователь биометрия-код. Нечеткий экстрактор, представляет из себя аналог кодов, обнаруживающих и исправляющих ошибки в векторе двоичных биометрических параметров. Нейросетевой преобразователь биометрия-код использует обученную ИНС для формирования точного значения ключа. Рассмотрим данные подходы более подробно.

1.5 Нечеткие экстракторы

Биометрическая система аутентификации на основе нечетких экстракторов также как и все рассматриваемые системы требует выполнения этапа регистрации пользователя. На этапе биометрической регистрации пользователя создается ключ *key*, который затем преобразуется в двоичный вектор *KEY* с использованием помехоустойчивых кодов таких, как Боуза-Чоудхури-Хоквингема (БЧХ) и Рида-Соломона:

$$KEY = Encode(key), \tag{1.1}$$

Большинство нечетких экстракторов строится на гаммировании [25]. Двоичный вектор *KEY* шифруется гаммированием, а в качестве гаммы используется вычисляемый в соответствии с полученной выборкой на этапе регистрации двоичный вектор биометрических параметров B:

$$T = B \oplus KEY, \tag{1.2}$$

где:

– знак $\oplus$ означает операцию побитового исключающего ИЛИ;

– T – двоичный вектор, результат выполнения операции гаммирования.

В открытом хелпере сохраняются T и $Hash(key)$ - хеш-сумма ключа key. Сам открытый хелпер помещается в базу данных открытых хелперов зарегистрированных пользователей.

В процессе биометрической аутентификации при предъявлении пользователем биометрических данных вновь вычисляется двоичный вектор биометрических параметров B'. Восстановление ключа key происходит с использованием открытого хелпера:

$$KEY' = T \oplus B' = KEY \oplus err, \tag{1.3}$$

где:

– err - ошибка, возникающая из-за разницы между двумя двоичными векторами биометрических параметров B и B', обуславливаемой неточностью воспроизведения биометрических данных. Таким образом, ключ key' необходимо обратно декодировать:

$$key' = Decode(KEY'), \tag{1.4}$$

Процедура аутентификация считается пройденной при выполнении равенства:

$$Hash(key') = Hash(key), \tag{1.5}$$

В случае неравенства хеш-сумм пользователь не проходит проверку его подлинности. На рисунке 1.4 и рисунке 1.5 показан принцип работы нечеткого экстрактора, использующего коды БЧХ для исправления ошибок err.

Для того чтобы считать преобразование с использованием нечеткого экстрактора надежным должно выполняться несколько условий. Во-первых, входной вектор двоичных биометрических параметров B должен иметь равновероятное распределение бит.

Во-вторых, входной вектор двоичных биометрических параметров должен содержать независимые (некоррелированные) данные. В-третьих, данные T, которые размещаются в открытом хелпере, не должны приводить к утечке криптографического ключа. В-четвертых, при предъявлении образов

«Чужой» преобразователь должен формировать случайную кодовую комбинацию.

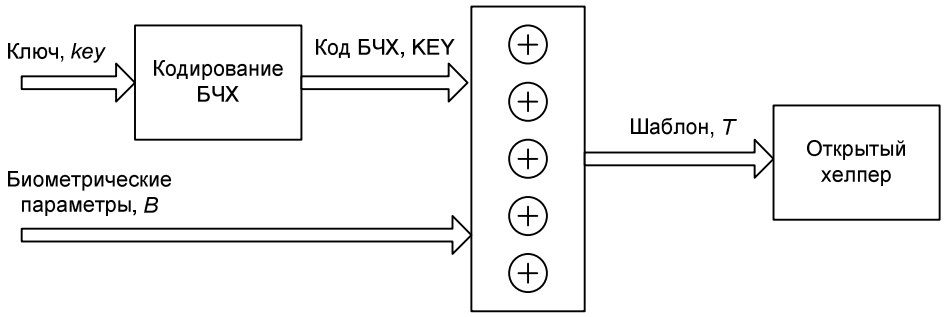

Рисунок 1.4 – Формирование открытого хелпера (регистрация биометрии)

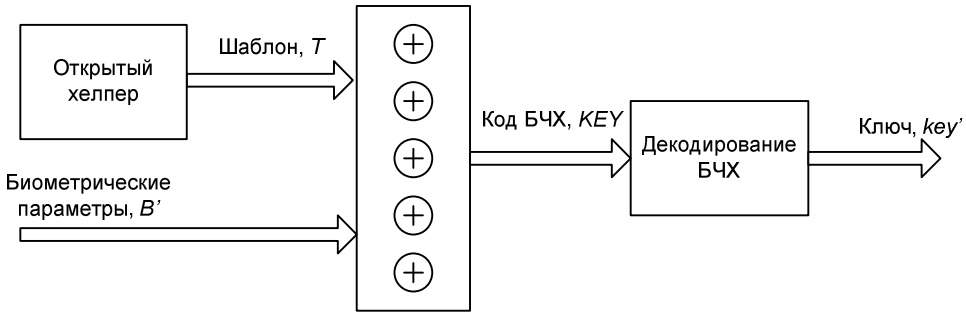

Рисунок 1.5 – Формирование ключа нечетким экстрактором с использованием биометрических данных и открытого хелпера

Вероятность ошибок первого рода P_I, то есть способность системы формировать ключ пользователя при предъявлении биометрического образа «Свой» существенно зависит от ошибки err. В одних из последних работах российских исследователей показано, что восстановление 25% ошибок оказывается недостаточным для полного восстановления ключа из вектора двоичных биометрических параметров. Для обеспечения уровня P_I меньше 0.1 исследователями вводится избыточность корректирующего кода, следовательно, его позиции становятся более зависимыми. Во многом завышенные оценки вероятности ошибок второго рода P_{II} разработчиками

систем биометрической аутентификации обусловлены тем, что не принимаются во внимание корреляционные связи биометрических параметров.

Попытки использования кодов с обнаружением и исправлением ошибок приводят к многократной избыточности двоичного вектора биометрических параметров B. Приходится применять коды с 90% избыточностью, теряя большую часть низкокачественных параметров (используется не более 10% входных параметров, имеющих достаточное качество).

Можно отметить несколько работ, в которых достаточно подробно описывается принцип построения нечетких экстракторов, связывающих биометрию и криптографию, то есть преобразующих биометрию в личный ключ пользователя.

Таким образом, структура нечеткого экстрактора представляет собой корректирующий код (БЧХ, Рида-Соломона), который стремится исправить ошибки, возникающие в биометрических параметрах, с целью дешифрования точного значения ключа с использованием открытого хелпера. Основная сложность, которая возникает при построении нечеткого экстрактора, заключается в создании алгоритма вычисления более устойчивых к шумам биометрических параметров рисунка отпечатка пальца. В настоящее время общепринятого подхода к созданию такого алгоритма не существует.

1.6 Нейросетевые преобразователи биометрия-код

Как уже было отмечено, нейросетевые преобразователи биометрия-код использует обученную ИНС для формирования точного значения ключа. На этапе биометрической регистрации пользователя создается ключ *key* и на этом ключе автоматически обучается ИНС без участия человека (учителя).

Стандарт ГОСТ Р 52633.5 – 2011 [16] предусматривает обучение однослойных и двухслойных ИНС. На рисунке 1.6 показана общая схема обучения.

Помимо ключа для обучения ИНС требуются выборки (примеры) двух классов образов – «Свой» и «Чужой», представленные в виде векторов биометрических параметров $V_{Св}$ и $V_{Чж}$ соответственно. Предусматривается обучение на непрерывных и дискретных биометрических параметрах.

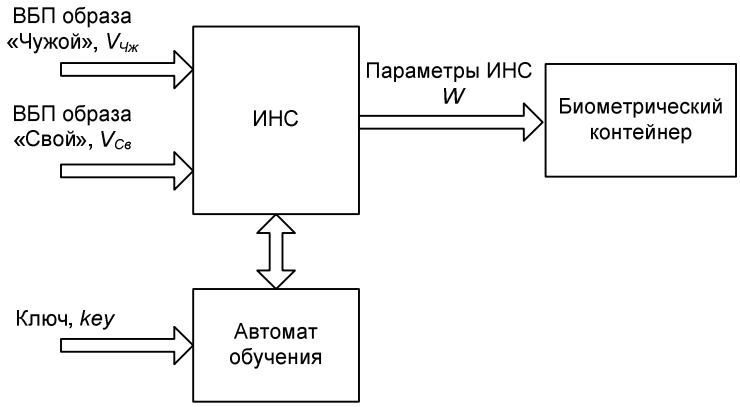

Рисунок 1.6 – Общая схема процедуры автоматического обучения нейросетевого преобразователя биометрия-код

Помимо ключа для обучения ИНС требуются выборки (примеры) двух классов образов – «Свой» и «Чужой», представленные в виде векторов биометрических параметров $V_{Св}$ и $V_{Чж}$ соответственно. Предусматривается обучение на непрерывных и дискретных биометрических параметрах.

Формально ИНС описывается матрицей весовых коэффициентов W или таблицами связей нейронов и таблицами весовых коэффициентов, которые помещаются в биометрический контейнер для последующего восстановления ключа. Процесс обучения ИНС необходим для вычисления W так, чтобы при воздействии на нее (подача на ее входы) примерами образа «Свой» на выходах ИНС формировалось точное значение ключа *key*. Общая схема нейросетевого преобразования биометрия-код представлена на рисунке 1.7. При воздействии на ИНС примерами образа «Чужой» на выходах ИНС должны формироваться случайные выходные коды.

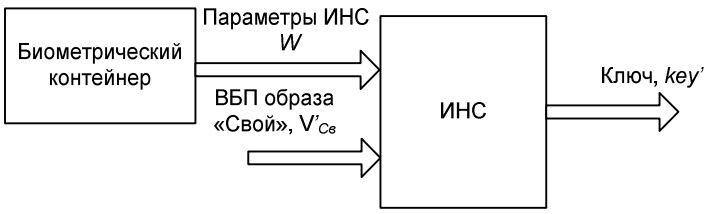

Рисунок 1.7 – Общая схема нейросетевого преобразования биометрия-код

Достоинством нейросетевых перобразователей биометрия-код считаются хеширующие свойства ИНС, которые могут быть значительно усилены механизмом размножения ошибок промежуточных кодов биометрических преобразований, основанном на сложении по модулю два данных еще не использованных нейронов с фрагментами уже полученного предшествующими нейронами выходного кода доступа или криптографического ключа.

1.7 Выводы по первому разделу

Проведен обзор основных видов биометрических систем, показавший, что их можно разделить на системы, в которых обрабатываются биометрические шаблоны, и системы, в которых обрабатываются биометрические контейнеры.

Проведен анализ зарубежных и отечественных технологий преобразования биометрических данных в код аутентификации (биометрия-код), который показал, что существует два основных направления решения задачи. Первое направление характеризуется использованием нечетких экстракторов на основе кодов с обнаружением и исправлением ошибок. Второе направление характеризуется применением больших искусственных нейронных сетей. Анализ литературы показал, что исследования нечетких экстракторов проходят преимущественно за рубежом. В РФ создано и активно развивается направление нейросетевого преобразования биометрических данных человека в код доступа.

Разработаны отечественные стандарты высоконадежной нейросетевой биометрической аутентификации. Тогда как нечеткие экстракторы

не являются стандартизированной технологией. Стандартов посвященных проектированию и разработке биометрических систем на основе нечетких экстракторов введено так и не было.

На основе нейросетевого преобразователя и нечеткого экстрактора могут быть разработаны способы обезличивания биометрических данных, которые позволили бы сделать невозможным определение принадлежности биометрического контейнера конкретному субъекту. Поэтому актуальными задачами являются разработка способов обезличивания биометрических данных и их моделирование.

2 Разработка способов обезличивания персональных данных в биометрических системах

2.1 Методы обезличивания персональных данных

2.1.1 Метод введения идентификаторов

К методам обезличивания, относятся:

– метод введения идентификаторов, в котором часть данных заменяется (значений ПДн) идентификаторами и создаётся таблица, в которой идентификаторы соответствуют исходным значениям;

– метод изменения состава или семантики, в котором с использованием замены результатов статистической обработки, преобразования, обобщения или удаления части ПДн, изменяется состав или семантика;

– метод декомпозиции, в котором множества ПДн разделяются на несколько подмножеств, которые раздельно хранятся ;

– метод перемешивания, в котором группы значений или отдельные значения атрибутов ПДн в массиве ПДн переставляются.

С применением одного из методов обезличивания получаются обезличенные данные, которые обладают различными свойствами, что осуществляет все виды обработки ПДн. Поэтому существуют условия, при описании методов, которые обеспечивают осуществление определенных свойств и требований.

Метод введения идентификаторов осуществляется путем замены части ПДн, которые позволяют идентифицировать субъект и создавать таблицы соответствия.

С применением метода появляется возможность получать обезличенные данные обладающие такими свойствами, как:

– полнота, в котором информация, позволяет идентифицировать субъекты ПДн, переносится в таблицу соответствия, а не удаляется;

– структурированность, при котором, после процедуры обезличивания,

каждому идентификатору соответствует свой набор данных;

– семантическая целостность, при котором представленные данные переносятся в таблицу соответствия.

Возможность обеспечения анонимности происходит при определенных условиях выбора идентификаторов и ПДн, которые они заменяют. Метод не постоянен к атакам, которые связаны со справочниками идентификаторов при косвенном деобезличивании и к атакам, связанными с деобезличиванием, которое использует информацию из справочников идентификаторов. Кроме того, при увеличении объема обезличиваемых данных стойкость метода не повышается.

Полученные в результате применения данного метода обезличенные данные, не обладают свойством релевантности, так как в запросе и в ответе на запрос изменяется вид представления ПДн, которые были заменены идентификаторами.

С применением этого метода появляется возможность сохранять в записях связи между атрибутами обезличенных данных, которые соответствуют связям между атрибутами ПДн.

Применение метода нужно осуществлять при малом количестве атрибутов ПДн и малом объеме массива ПДн, так как объем справочников зависит от этих параметров. Если часто вносить изменения в состав данных и значения атрибутов, то вычислительная эффективность метода будет снижена.

2.1.2 Метод изменения состава или семантики

Метод изменения состава или семантики осуществляется с помощью сложения, изменения значений атрибутов ПДн или удаления информации, которая позволяет распознать субъект.

С применением метода появляется возможность получать обезличенные данные, обладающие такими свойствами, как:

– структурированность, при котором не нарушается связь между

отдельными значениями атрибутов ПДн субъекта;

– анонимность, при котором к неоднозначности, при идентификации с применением обезличенных данных, приводит удаление или сложение некоторых данных.

Свойство полноты имеют полученные обезличенные данные при проведении изменений в составе ПДн, которые сохраняют данные. У полученных обезличенных данных уменьшается свойство полноты, если удалить части сведений.

Если провести изменения в составе ПДн, которые сохраняют семантику данных, то обеспечивается семантическая целостность полученных данных.

В том числе обеспечиваются такие свойства обезличенных данных, как:

– частичная релевантность, так как иногда получают семантическое соответствие поискового запроса и полученного ответа на запрос;

– применимость, так как оператор может выполнить обработку, которая не требует деобезличивания всего объема данных о субъектах.

Нужно учитывать вероятность проведения обезличивания с применением данных атрибутов, при выделении атрибутов ПДн. Обезличивание может не выполниться, в случае простого изменения значений отдельных атрибутов, так как выполнится только изменение состава ПДн.

С применением метода появляется возможность частично сохранять в записях связи между атрибутами обезличенных данных, которые имеют соответствия связям между атрибутами ПДн.

Данный метод применяется в случае, когда возможно изменение состава и семантики, так, что задачи обработки ПДн не требуют деобезличивания, так как метод не обладает свойством обратимости при любых изменениях состава и семантики данных. Иначе необходимо использовать дополнительную информацию для проведения деобезличивання.

Также метод применяется, когда оператор использует автономно

обезличенные данные, и когда несовместимы с данными других операторов.

2.1.3 Метод декомпозиции

Метод декомпозиции осуществляется с помощью разделения множества атрибутов ПДн на несколько подмножеств и создания таблиц, которые устанавливают связи между подмножествами, с последующим раздельным хранением записей, которые соответствуют подмножествам этих атрибутов.

С применением метода появляется возможность получать обезличенные данные, обладающие такими свойствами, как:

– полнота, при котором информация о субъектах ПДн переносится в другое хранилище, а не удаляется;

– структурированность, при котором сохраняется связь между записями в разных хранилищах, которое позволяет однозначно сопоставить их;

– семантическая целостность, при котором не изменяется семантика и вид представления данных о субъекте.

При сложных связях между хранилищами и защите хранилищ от НСД выполняется анонимность, так как метод не устойчив к атакам, которые направленны на деобезличивание путем анализа данных из различных хранилищ и косвенному деобезличиванию.

Также обеспечиваются такие свойства обезличенных данных, как:

– релевантность, так как возможно получить семантическое соответствие поискового запроса и полученного ответа на запрос;

– применимость, так как оператор выполняет обработку данных, которые располагаются в одном хранилище, как независимо от другого, так и при совместном их использовании, без деобезличивания всего объема обезличенных данных.

С применением метода появляется возможность сохранять в записях каждого хранилища связи между атрибутами обезличенных данных,

соответствующие связям между атрибутами ПДн.

Данный метод применяется при значительном количестве атрибутов ПДн, но при не частом внесении изменений в состав данных и значения атрибутов.

2.1.4 Метод перемешивания

Метод осуществляется с помощью перемешивания между собой отдельных значений или групп значений атрибутов ПДн.

С применение метода появляется возможность получать обезличенные данные, обладающие такими свойствами, как:

– полнота, при котором сохраняется вся информация о субъектах ПДн;

– структурированность, в котором, при деобезличивании, связи между данными полностью восстанавливаются;

– семантическая целостность, при котором не изменяется семантика и вид представления данных о субъекте;

– анонимность, при котором перемешиваются данные по каждому отдельному атрибуту записи о субъекте, что не позволяет без доступа к дополнительной информации определить принадлежность тех или иных данных конкретному субъекту.

Также обеспечиваются такие свойства обезличенных данных, как:

– релевантность, так как есть возможность получать семантическое соответствие поискового запроса и полученного ответа на запрос;

– применимость, так как оператор может выполнять обработку как отдельных записей о субъектах, так и всех данных, без деобезличивания всего объема обезличенных данных, при наличии доступа к дополнительной информации.

С применение метода не сохраняются в записях связи между атрибутами обезличенных данных, которые соответствуют связям между атрибутами ПДн.

Данный метод применяется при значительном количестве атрибутов

ПДн и большом объеме массива ПДн, так как стойкость метода к атакам направленным на деобезличивание увеличивается с увеличением указанных параметров, а количество дополнительной информации слабо зависит от объема массива ПДн.

2.2 Вычисление биометрических параметров отпечатка пальца

2.2.1 Двоичные биометрические параметры

Наиболее информативными особенностями отпечатка пальца являются контрольные точки: окончания гребней, разветвления гребней. Взаимное расположение таких точек представляет уникальную информацию, по которой можно однозначно идентифицировать человека.

а) разветвление б) окончание

Рисунок 2.1 – Два типа особых точек на папиллярном рисунке отпечатка пальца

Контрольные точки можно описать их набором из 4 параметров:

а) координата *x*;

б) координата *y*;

в) направление папиллярной линии в точке θ;

г) тип точки *t*.

Сам отпечаток пальца можно описать как множество контрольных точек:

$$T = \{m_1, m_2, ..., m_k\}, m_i = \{x_i, y_i, \theta_i, t_i\}, i = 1...k\,, \quad (2.1)$$

где:

– m_i - контрольная точка, обнаруженная на изображении отпечатка пальца;

– k - число контрольных точек.

Множество контрольных точек T есть биометрический шаблон, который может быть использован для сравнения с другими образцами. Процесс сравнения ведется путем сопоставления всевозможных пар контрольных точек, содержащихся в шаблоне, и точек образца. Коэффициент соответствия двух отпечатков пальцев определяется по формуле:

$$K = \frac{D^2}{T \cdot S} \cdot 100\%, \tag{2.2}$$

где:

– D - количество совпавших контрольных точек;

– T - количество контрольных точек в шаблоне;

– S - количество контрольных точек в образце или идентифицируемом отпечатке пальца.

Отпечатки считаются идентичными при K больше 65%. Хранение биометрического шаблона в базах данных несет в себе потенциальную угрозу безопасности биометрических данных. Потеря конфиденциальности биометрического шаблона будет означать, что конфиденциальность данных потеряна навсегда. Биометрический шаблон содержит уникальные параметры человека в чистом виде и, оказавшись в руках у злоумышленника, дает ему возможность для осуществления взлома биометрических систем и получения ценных сведений о человеке.

Расположение контрольных точек относительно друг друга может быть описано дискретным биометрическим параметром в виде матрицы позиций.

Рисунок отпечатка пальца с выделением фрагментов, где находятся особые точки и соответствующая их расположению матрица представлен на рисунке 2.2.

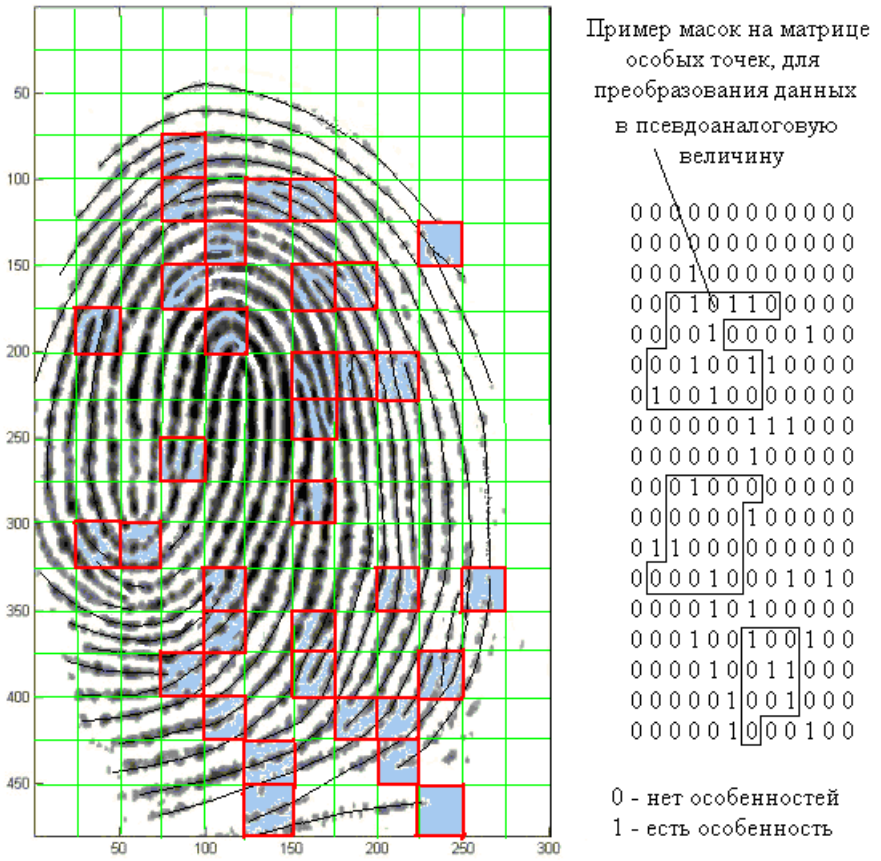

Рисунок 2.2 – Рисунок отпечатка пальца с выделением фрагментов, где находятся особые точки и соответствующая их расположению матрица

Возможно использование различных алгоритмов сравнений предъявленного рисунка отпечатка пальца и эталонного рисунка. Самым простым является сравнение матриц особенностей, представленное на правой части рисунка 2.2. При необходимости дискретные биометрические параметры могут быть переведены в непрерывные.

2.2.2 Непрерывные биометрические параметры

При распознавании отпечатков пальцев с помощью искусственной нейронной сети, уникальные особенности – совокупность контрольных точек и направления папиллярных линий могут быть представлены пространственно-частотными компонентами в горизонтальном и вертикальном измерениях. Данное решение позволяет получить параметры, которые описываются непрерывным множеством возможных значений. Пространственно-частотные компоненты широко применяются в методах

сжатия изображений и вычисляются с помощью двумерных дискретных преобразований. Рассмотрим двумерные дискретные преобразования, которые могут быть применены для представления отпечатка пальца в виде набора параметров и обучения искусственной нейронной сети.

Известным семейством двумерных дискретных преобразований являются дискретное косинус-преобразование, преобразование Кархунена-Лоэве, преобразование Уолша-Адамара, преобразование Хаара.

Дискретное косинус-преобразование (DCT, discrete cosine transform) является ортогональным преобразованием, тесно связано с дискретным преобразованием Фурье и достаточно изучено. Весьма эффективно применяется в таких методах сжатия изображений, как JPEG и MPEG.

Преобразование Кархунена-Лоэве (KLT, Karhunen-Loeve transform) считается теоретически наилучшим с точки зрения концентрации энергии. Однако его коэффициенты зависят от исходных данных, и их вычисление проходит медленно. По этим причинам метод KLT весьма редко применяется на практике.

Преобразование Уолша-Адамара (WHT, Walsh-Hadamard transform) быстро вычисляется. Преобразование довольно просто реализуется аппаратно, так как используется только сложение и вычитание значений данных. Однако по своим свойствам оказывается чуть хуже DCT.

Преобразование Хаара является вейвлетным преобразованием, которое используется в методах сжатия изображений, в основном цветных и черно-белых с плавными переходами.

В качестве функционалов используются методы DCT и WHT, так как предпочтение, прежде всего, отдается использованию известных и простых в реализации преобразований.

Двумерное DCT изображения позиций контрольных точек вычисляется по формулам:

$$D_{ij} = \frac{1}{\sqrt{2n}} C_i C_j \sum_{x=0}^{n-1} \sum_{y=0}^{n-1} B_{uv} \cos\left(\frac{(2y+1)j\pi}{2n}\right) \cos\left(\frac{(2x+1)i\pi}{2n}\right), \quad (2.3)$$

$$C_f = \begin{cases} \frac{1}{\sqrt{2}}, & f = 0 \\ 1, & f > 0 \end{cases}, \quad (2.4)$$

где:

– *0* меньше либо равно *i*, *j* меньше либо равно *n-1*,

– B_{uv} - изображение позиций контрольных точек размерности $n \times n$. Метод DCT можно интерпретировать с помощью базиса в *n*-мерном векторном пространстве. Так для *n* равно 16 получается 256 базисов.

Двумерное WHT вычисляется по формуле:

$$G_{ij} = \frac{1}{N} \sum_{x=0}^{n-1} \sum_{y=0}^{n-1} B_{xy} (-1)^{\sum_{i=0}^{m} [b_i(x) p_i(u) + b_i(y) p_i(v)]}, \quad (2.5)$$

где:

– *n* равно 2^m - степень двойки,

– величина $b_i(u)$ равна биту i в двоичном представлении целого числа u, а $p_i(u)$ определяется с помощью $b_j(u)$ из следующих рекуррентных соотношений:

$$\begin{aligned} &p_0(u) = b_{n-1}(u), \\ &p_1(u) = b_{n-1}(u) + b_{n-2}(u), \\ &p_2(u) = b_{n-2}(u) + b_{n-3}(u), \\ &\ldots \\ &p_{n-1}(u) = b_1(u) + b_0(u). \end{aligned} \quad (2.6)$$

При *n* равным 16 получается 256 базисов WHT.

Преобразование матрицы из 256 элементов дает столько же пространственно-частотных коэффициентов. Размерность вектора

непрерывных биометрических параметров должна быть подобрана исходя из обобщающей способности искусственной нейронной сети.

Таким образом, отпечаток пальца можно представить пространственно-частотными компонентами с помощью двумерного дискретного преобразования, учитывающего изменение координат контрольных точек и их взаиморасположение по двум измерениям (x,y). Базисные изображения дают понять, что получаемые значения коэффициентов зависимы от смещения и поворота контрольных точек на изображении, которые возникают при сканировании отпечатка пальца. Высокая величина дисперсии биометрических параметров может являться причиной низкой обобщающей способности искусственной нейронной сети, обученной на выборке образа «Свой». Дисперсия биометрических параметров обусловлена смещением контрольных точек на изображении, получаемом при сканировании отпечатка пальца.

Для исследования характеристик непрерывных биометрических параметров рисунка отпечатка пальца была сформирована база из 100 биометрических образов «Свой» и база «все Чужие», содержащая 100 отпечатков пальцев разных людей.

Как правило, биометрические данные неточно воспроизводимы, и это приводит к вариации вычисляемых параметров. Например, деформация кожи приводит к тому, что часть особенностей может быть не обнаружена на одном изображении рисунка отпечатка пальца и обнаружена на другом. Известно, что погрешность определения математических ожиданий и стандартных отклонений биометрических параметров влияет на ошибку обучения.

На рисунках 2.3 и 2.4 представлены гистограммы распределения различных параметров (20-й, 30-й, 60-й и 81-й параметр) образов «Свой» и «все Чужие» отпечатка пальца, показан график нормального распределения, построенный для вычисленных значений математического ожидания и стандартного отклонения.

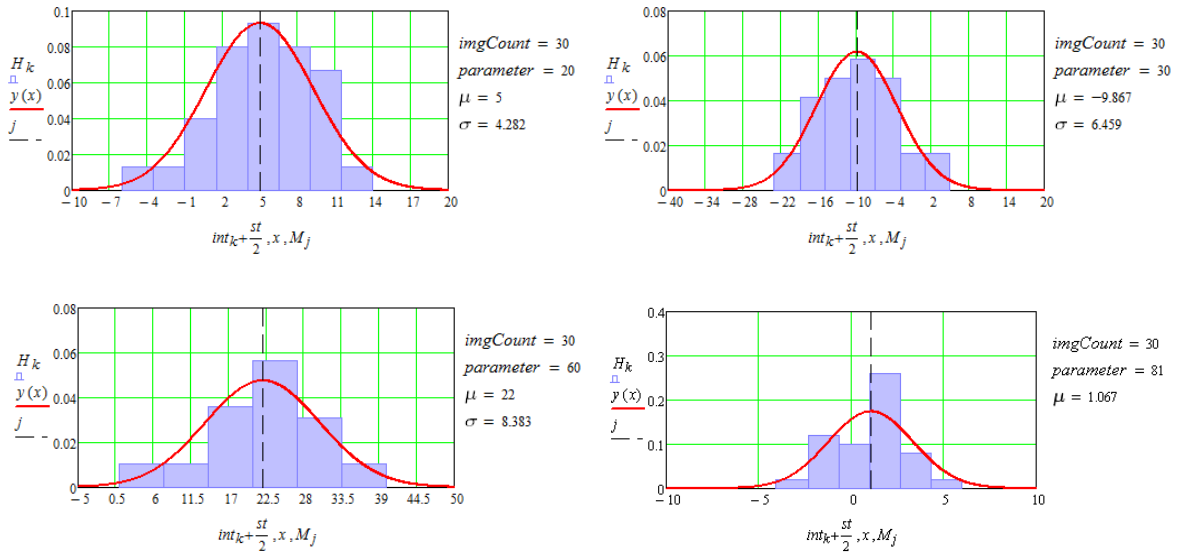

Рисунок 2.3 – Гистограммы распределений биометрических параметров образа «Свой»

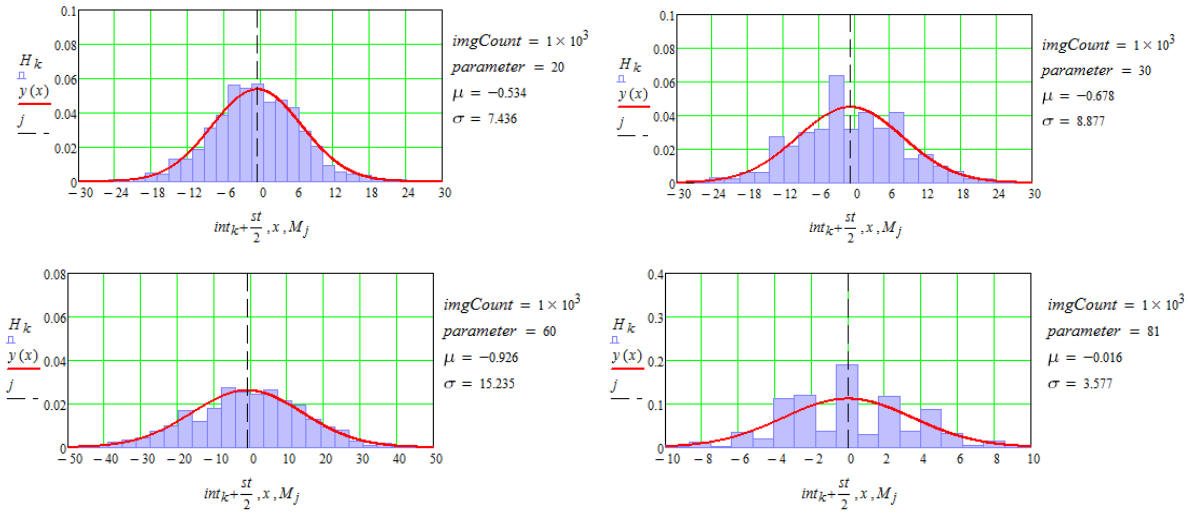

Рисунок 2.4 – Гистограммы распределений биометрических параметров образа «все Чужие»

На рисунке 2.5 представлен график плотности вероятности распределения одного биометрического параметра для пользователей «Свой», «Чужой 1», «Чужой 2», «Чужой 3», «Чужой 4» и «все Чужие».

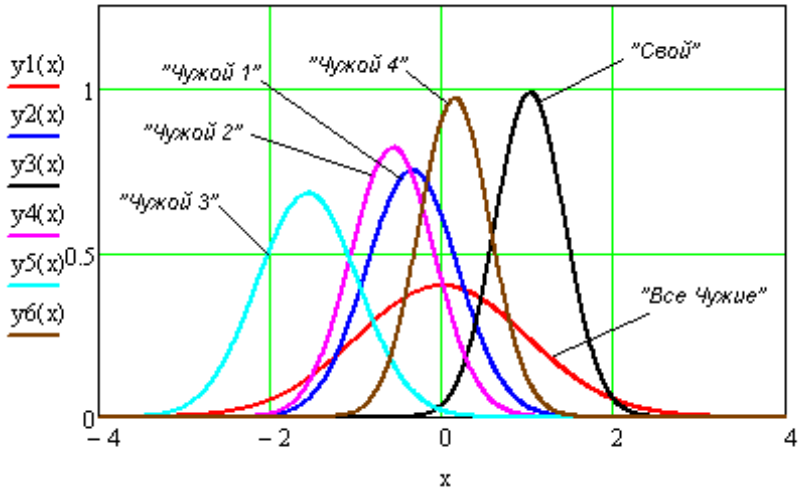

Рисунок 2.5 – Распределения биометрического параметра различных образов «Свой», «Чужой 1», «Чужой 2», «Чужой 3», «Чужой 4» и «все Чужие»

Из рисунка видно, что распределения биометрических параметров, описываемые нормальным законом распределения, существенно различаются. Математические ожидания параметров различных образов оказывается разнесенными в области значений «все Чужие».

Корреляционный анализ непрерывных биометрических параметров образов «все Чужие» рисунка отпечатка пальца показал, что математическое ожидание модулей коэффициентов парной корреляции $E\left(\left|r_{v_i,v_j}\right|\right)$ приблизительно равно 0,1. Оценка корреляционных связей биометрических параметров образа «Свой» показала, что коэффициент корреляции между парами входных биометрических параметров образа «Свой» является случайной величиной, хорошо описываемой нормальным законом распределения значений. И математическое ожидание модулей парной корреляции $E\left(\left|r_{v_i,v_j}\right|\right)$ составляет значительную величину от 0,2 до 0,6 (см. рисунок 2.6).

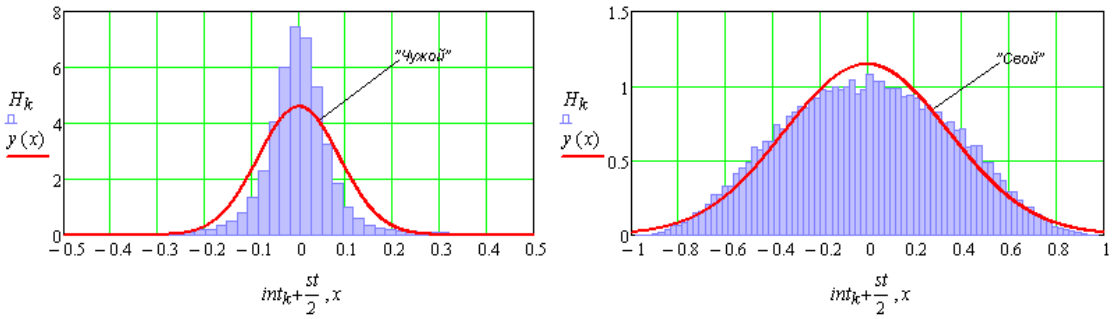

Рисунок 2.6 – Гистограммы распределений коэффициентов парной корреляции

2.3 Способ обезличивания персональных данных с использованием нейросетевого преобразователя биометрия-код

Анализ методов обезличивания и их алгоритмов показал, что процесс можно описать как разделение множества атрибутов ПДн субъекта P на два подмножества – идентифицирующих данных P_1 и обезличенных данных P_2:

$$P_1=\{d_{11},d_{12},\ldots,d_{1m}\}; \quad (2.7)$$

$$P_2=\{d_{21},d_{22},\ldots,d_{2n}\}; \quad (2.8)$$

$$P=P_1 \cup P_2. \quad (2.9)$$

Подмножество идентифицирующих данных P_1 содержит данные, по которым субъект может быть однозначно идентифицирован. Подмножество обезличенных данных P_2 не позволяет однозначно идентифицировать субъекта, тем самым обеспечивает анонимность обрабатываемых сведений. Деобезличивание заключается в объединении двух подмножеств, результат которого позволяет определить принадлежность обезличенных данных по конкретному субъекту.

Для сохранения анонимности обезличенных данных предлагается вместо деобезличивания использовать биометрическую аутентификацию, для чего в подмножество обезличенных данных следует включить данные защищенного биометрического контейнера B. Алгоритм обезличивания ПДн с использованием нейросетевого преобразователя биометрия-код представлен на рисунке 2.7.

Полученные ПДн субъекта обезличиваются с помощью одного или нескольких методов: метода введения идентификаторов, метода изменения состава или семантики, метода декомпозиции, метода перемешивания. В результате образуются идентифицирующие и обезличенные данные. Биометрические данные обезличиваются по одному из методов. Для чего субъект предъявляет несколько примеров биометрического образа «Свой», тем самым формируя обучающую выборку. Затем вычисляются ВНБП и автоматически обучается ИНС на случайно сгенерированном двоичном ключе. По окончании обучения создается защищенные биометрический контейнер *B*, содержащий идентификатор (псевдоним) субъекта *Id*, матрицу весовых коэффициентов *W* и *Hash* – значение хеш-функции от личного ключа (кода доступа) субъекта. Содержимое биометрического контейнера включается в обезличивание данных, обрабатываемые оператором ИСПДн, то есть *B* является подмножеством P_2.

Обезличенные данные являются анонимными, что позволяет предотвратить несанкционированное использование ПДн и снизить ущерб от возможного разглашения сведений о гражданах, обрабатываемых оператором.

Для определения принадлежности обезличенных данных конкретному субъекту без доступа к идентифицирующим данным и потери анонимности в соответствии с алгоритмом обезличенные данные находятся по идентификатору *Id*. Затем субъект предъявляет изображение отпечатка путем прикладывания к сканеру пальца. Далее вычисляется ВНБП, а параметр *W* используется для преобразования ВНБП в личный ключ (код доступа) субъекта с помощью ИНС. Алгоритм деобезличивания ПДн с использованием нейросетевого преобразователя представлен на рисунке 2.8.

Решение о принадлежности данных определяется по результату сравнения значения хеш-функции от сформированного ключа и значения *Hash*, содержащегося в обезличенных данных. Если значения совпадают, то делается вывод о том, что обезличенные данные принадлежат субъекту. Если значения не совпадают, то делается вывод о непринадлежности обезличенных

данных субъекту.

Таким образом, при B является подмножеством P_2 принадлежность обезличенных данных субъекту может быть определена без доступа к идентифицирующим данным и процедуры деобезличивания. За счет введения биометрической аутентификации анонимность обезличенных данных сохраняется. Доступ к идентифицирующим данным может быть предоставлен только ограниченному числу сотрудников оператора при отсутствии возможности осуществления биометрической аутентификации субъекта.

2.4 Способ обезличивания персональных данных с использованием нечеткого экстрактора

Алгоритм обезличивания ПДн с использованием нечеткого экстрактора представлен на рисунке 2.9.

Полученные ПДн субъекта обезличиваются с помощью одного или нескольких методов: метода введения идентификаторов, метода изменения состава или семантики, метода декомпозиции, метода перемешивания. В результате образуются идентифицирующие и обезличенные данные. Биометрические данные обезличиваются с использованием нечеткого экстрактора. Для чего субъект предъявляет несколько примеров биометрического образа «Свой». Затем вычисляются векторы двоичных биометрических параметров. Далее создается случайный ключ, который затем преобразуется в двоичный вектор с использованием помехоустойчивого кода БЧХ. Далее двоичный вектор шифруется гаммированием, а в качестве гаммы используется вычисляемый двоичный вектор биометрических параметров. В результате создается защищенные биометрический контейнер B, содержащий идентификатор (псевдоним) субъекта Id, результат гаммирования T и $Hash$ – значение хеш-функции от личного ключа (кода доступа) субъекта. Содержимое биометрического контейнера включается в обезличивание данных, обрабатываемые оператором ИСПДн, то есть B

является подмножеством P_2.

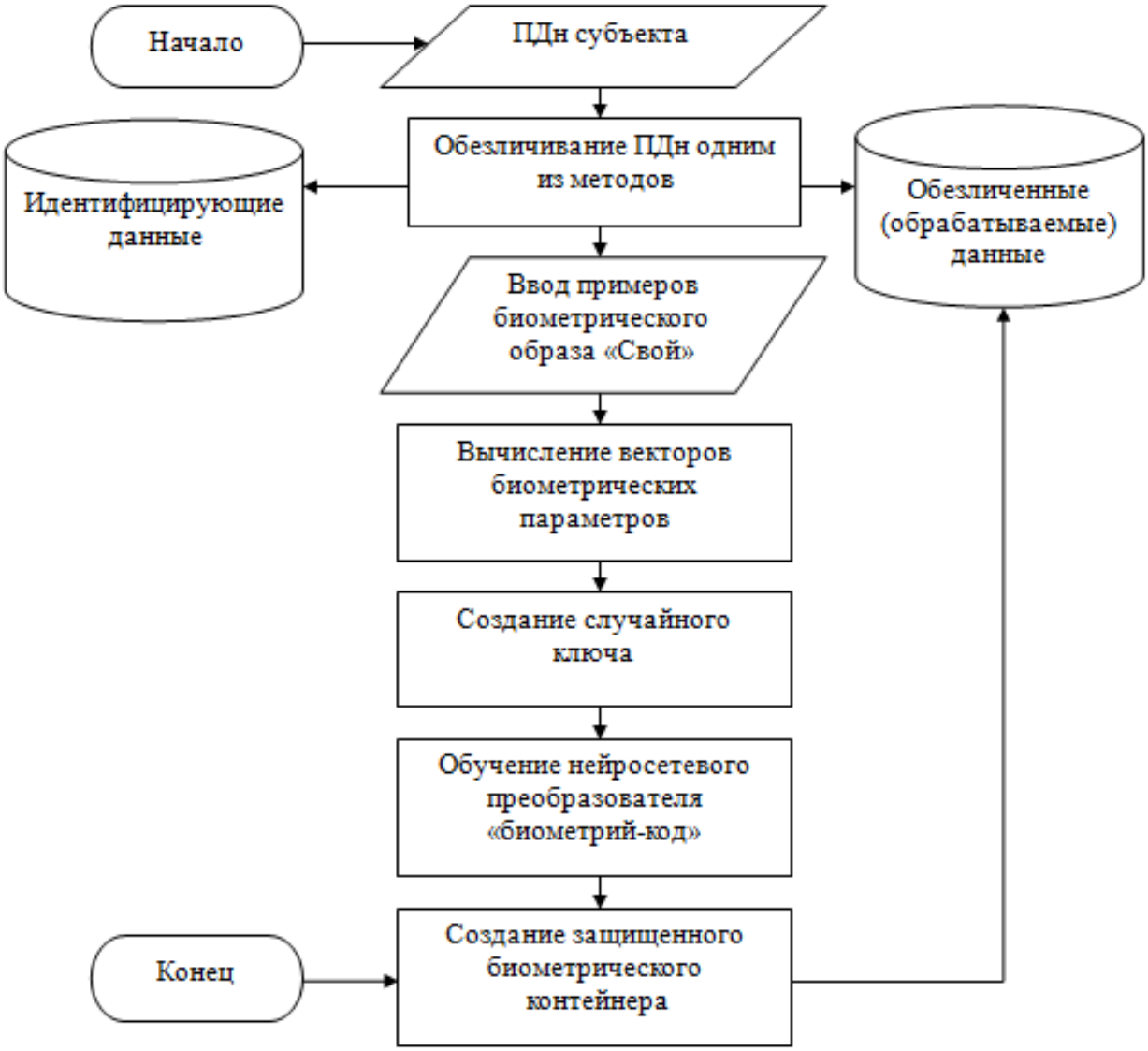

Рисунок 2.7 - Алгоритм обезличивания ПДн с использованием нейросетевого преобразователя

Рисунок 2.8 - Алгоритм деобезличивания ПДн с использованием нейросетевого преобразователя

Для определения принадлежности обезличенных данных конкретному субъекту без доступа к идентифицирующим данным и потери анонимности в соответствии с алгоритмом деобезличивания ПДн с использованием нечеткого экстрактора, представленном на рисунке 2.10, обезличенные данные находятся по идентификатору *Id*. Затем субъект предъявляет изображение отпечатка путем прикладывания к сканеру пальца. Вычисляется вектор двоичных биометрических параметров, затем выполняется гаммирование с использованием *T*. Далее осуществляется декодирование результата гаммирования, так как он содержит ошибку, вносимую биометрическими данными. Затем формируется хеш-функция от ключа, полученного в результате декодирования.

Решение о принадлежности данных определяется по результату

сравнения значения хеш-функции от сформированного ключа и значения *Hash*, содержащегося в обезличенных данных. Если значения совпадают, то делается вывод о том, что обезличенные данные принадлежат субъекту. Если значения не совпадают, то делается вывод о непринадлежности обезличенных данных субъекту.

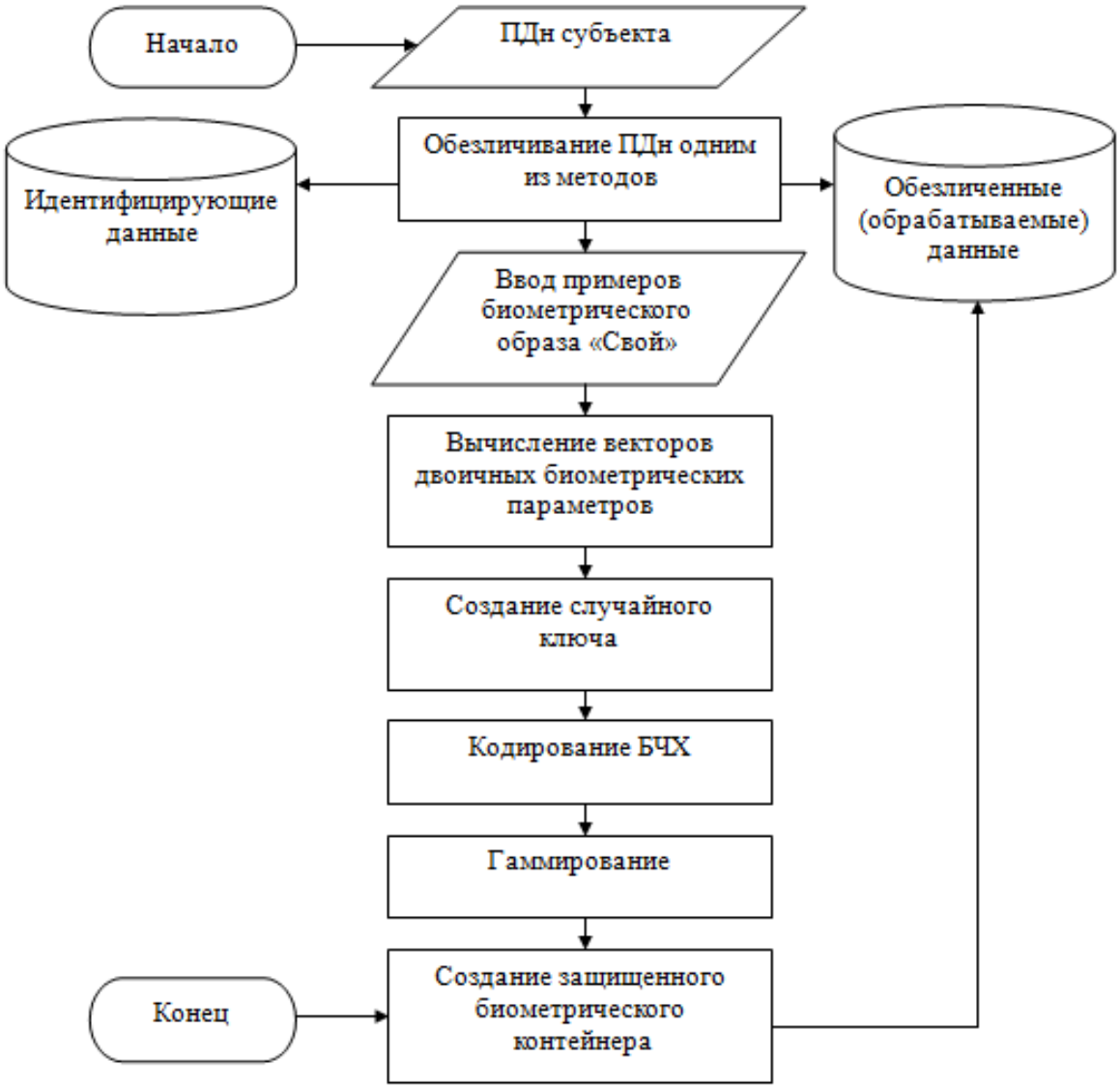

Рисунок 2.9 - Алгоритм обезличивания ПДн с использованием нечеткого экстрактора

Рисунок 2.10 - Алгоритм деобезличивания ПДн с использованием нечеткого экстрактора

2.5 Выводы по второму разделу

Существующие методы обезличивания персональных данных имеют недостаток, заключающийся в необходимости использования при обработки операторами сведений, идентифицирующих человека и удостоверяющих его личность.

Разработаны способы обезличивания персональных данных в биометрических системах. В первом способе используется нейросетевой преобразователь биометрия-код. Второй способ отличается использованием нечеткого экстрактора.

Представлены алгоритмы обезличивания персональных данных, в которых полученные ПДн субъекта обезличиваются с помощью одного или нескольких традиционных методов, а биометрические данные обезличиваются с помощью нейросетевого преобразователя или нечеткого экстрактора.

Включение биометрического контейнера в обезличенные данные позволяет ограничить доступ операторам к информации, идентифицирующей человека, а принадлежность обезличенных данных конкретному субъекту определять с помощью биометрической аутентификации.

3 Моделирование способов обезличивания персональных данных в биометрических системах

3.1 Программная среда сбора отпечатков пальцев

Программное обеспечение предназначено для организации сбора биометрических данных (отпечатков пальцев) человека. Обеспечивает выполнение следующих функций:

– контроль корректного ввода образов.

– загрузку ранее созданной базы.

Для полноценной работы ПО на компьютер был установлен сканер отпечатков пальцев Futronic FS80 с соответствующими для него драйверами.

Установка драйвера.

При подключении сканера Futronic FS80 ОС обнаружило новое устройство и запустило «Мастер нового оборудования». Далее следуем инструкциям «Мастера нового оборудования», представленным на рисунке 3.1.

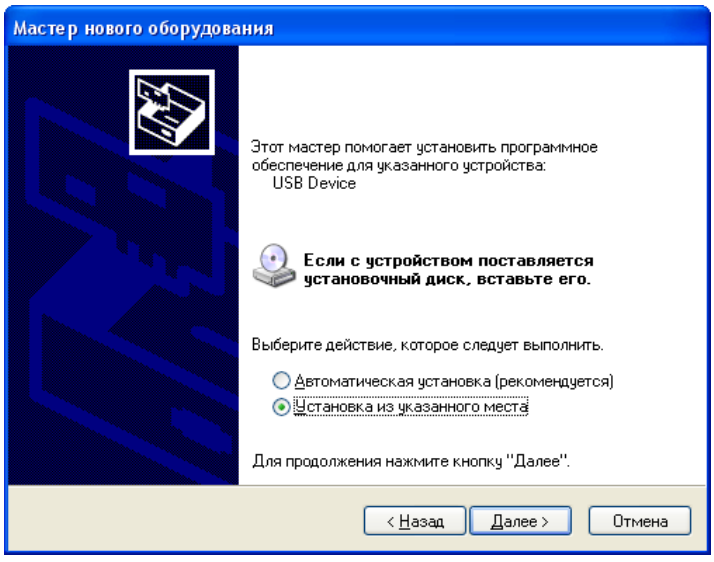

Рисунок 3.1 - Инструкции «Мастера нового оборудования»

В ходе его работы было предложено два варианта установки драйвера, либо автоматическая, либо установка из указанного места. Так как сканер не

был установлен ранее, то ОС не нашла драйвер автоматически. При наличии CD-диска производителя с драйвером оборудования был выбран пункт «Установка из указанного места». В следующем окне выбрано расположение драйвера производителя, представленное на рисунке 3.2.

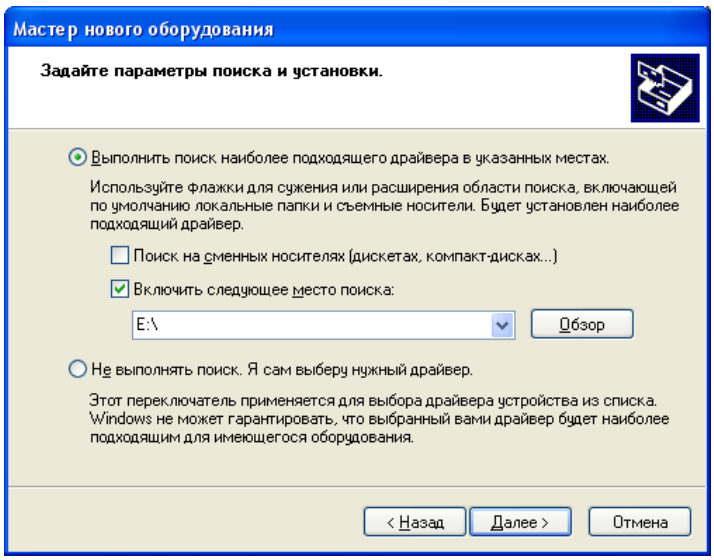

Рисунок 3.2 – Расположение драйвера производителя

Следуя инструкциям, драйвер установился в систему, и «Мастер нового оборудования» завершил свою работу, представленную на рисунке 3.3.

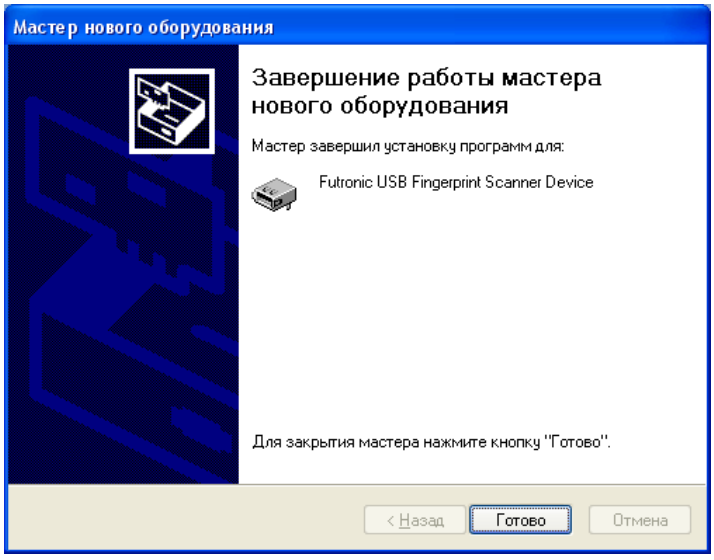

Рисунок 3.3 – Завершение работы мастера нового оборудования

Вызов и загрузка программы.

Для вызова и загрузки программы осуществлен переход в папку с программой на жестком диске и запущен файл fingerProj.exe. В результате выполнения программы на экране видеомонитора отобразилось главное окно модуля формирования баз отпечатков.

Описание режимов работы программы.

Общий вид программы формирования баз отпечатков представлен на рисунке 3.4.

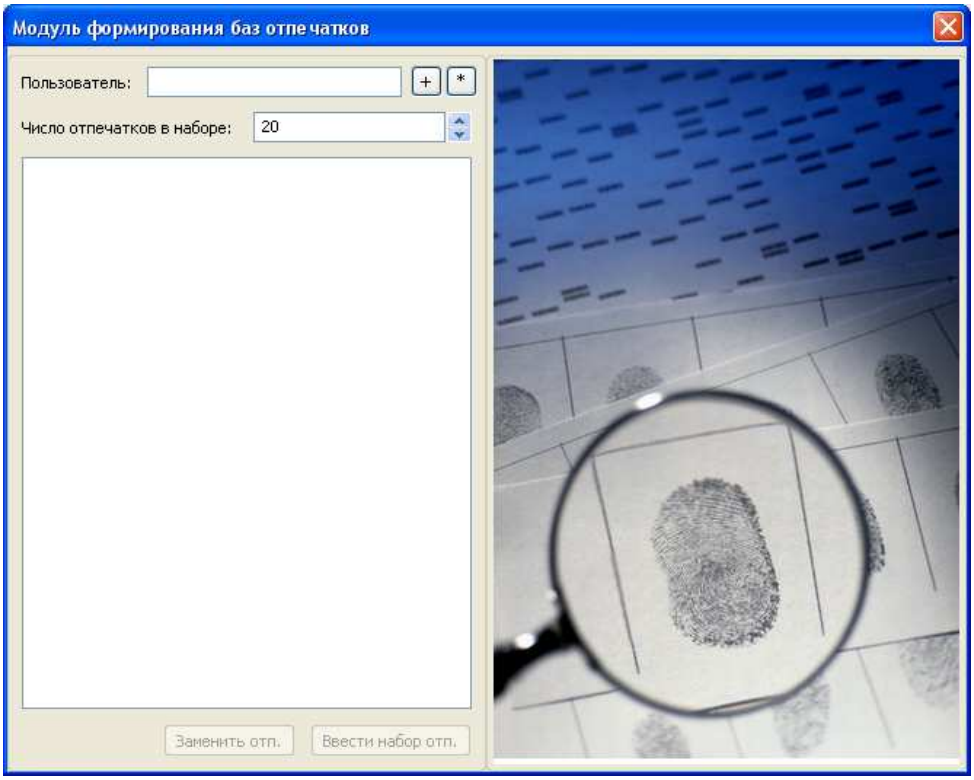

Рисунок 3.4 - Общий вид программы формирования баз отпечатков

В левой части главного окна программы располагается область, в которую вводится информация о пользователе и его образах. В правой части содержится окно для просмотра сохраненных образов баз отпечатков.

Программа позволяет создать новую базу биометрических данных или редактировать уже существующую. Формирование базы осуществляется добавлением пользователя и захвата изображений его отпечатков пальцев со сканера. Файлы базы сохраняются в рабочей папке с программой.

Добавление нового пользователя.

Для добавления нового пользователя в поле «Пользователь» было указано имя пользователя.

В поле «Число образов» введено количество вводимых образов одного пальца.

По умолчанию поле «Число образов» принимает значение 20. Минимальное число вводимых образов одного пальца равно 8. Максимальное число вводимых образов одного пальца равно 40.

После нажатия «+» новый пользователь был добавлен в дерево каталогов. Дерево каталогов служит для повышения навигации пользователей в среде и содержит списки образов пальцев пользователей, которые необходимо ввести или заменить.

Добавление нового пользователя представлено на рисунке 3.5.

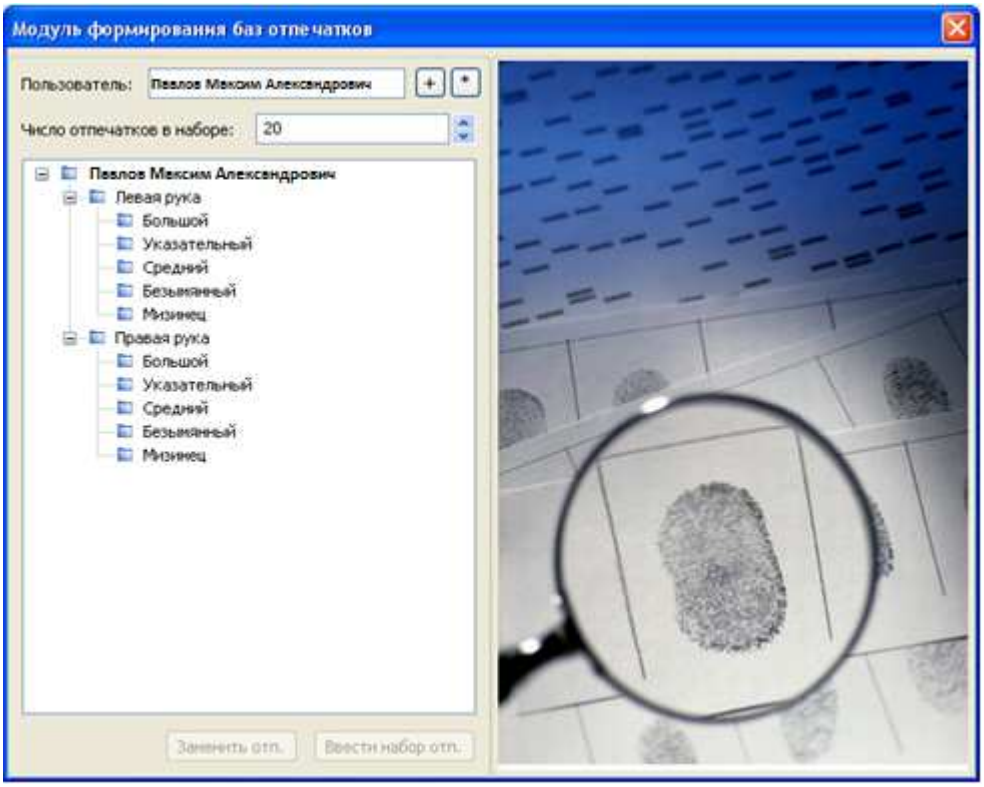

Рисунок 3.5 – Добавление нового пользователя

Сканирование отпечатков пальцев.

После добавление нового пользователя в дерево каталогов баз отпечатков был выбран подкаталог «Левая рука». Указан подкаталог соответствующий названию пальца выбранной руки. При нажатии «Ввести набор отп.». запущена процедура захвата набора образов выбранного пальца, представленная на рисунке 3.6.

Аналогичные действия произведены при выборе подкаталога «Правая рука».

Рисунок 3.6 – Процедура захвата набора образов выбранного пальца

В левой части окна программы располагается область, в которой выводится информация о пользователе и состояние ввода его образов. Индикатор прогресса показывает ход процесса формирования базы. В правой части окна программы находится область вывода захваченного изображения со сканера отпечатков пальцев, а также вывод графических сообщений. Сообщения уведомляют пользователя о необходимости корректного расположения пальца на датчике.

После появления сообщения «ПРИЛОЖИТЕ ПАЛЕЦ К ДАТЧИКУ» палец был расположен на сканере и прижат с небольшим усилием. Захваченное изображение отпечатка должно находиться во внутренней рамке и преимущественно по центру. Если захват отпечатка пальца не происходит, то следует:

– прижать сильнее палец при появлении сообщения «ПРИЛОЖИТЕ ПАЛЕЦ СИЛЬНЕЕ», как представлено на рисунке 3.7;

Рисунок 3.7 – «Приложите палец сильнее»

– сместить расположение пальца при появлении сообщений «ПЕРЕМЕСТИТЕ ПАЛЕЦ ВЛЕВО» или «ПЕРЕМЕСТИТЕ ПАЛЕЦ ВПРАВО» в направлении указанной стрелки, представлено на рисунке 3.8;

Рисунок 3.8 – Смещение расположения пальца

– повернуть палец вертикально при появлении сообщения «ПОВЕРНИТЕ ПАЛЕЦ ВЕРИТИКАЛЬНО», так чтобы края отпечатка были условно параллельны рамке окна и симметричны относительно друг друга, представлено на рисунке 3.9;

Для меньшей деформации отпечатка пальца при перемещении рекомендуется его последовательно отрывать и прикладывать к сканеру. Перекатывание сильно деформирует рисунок папиллярных линий, что может повлиять на качество базы.

Местонахождение пальца на сканере удовлетворено требованиям расположения, образ был захвачен. При завершении сканирования определенного числа образов отпечатка пальца появилось информационное сообщение «Отпечатки сохранены», представленное на рисунке 3.10.

Рисунок 3.9 – «Поверните палец вертикально»

Рисунок 3.10 – Завершение сканирования

Список захваченных образов отпечатка пальца был сформирован в подкаталоге соответствующего пальца. Для создания полной базы биометрических данных было произведено сканирование для каждого пальца пользователя.

Загрузка существующей базы отпечатков пальцев.

При изменении (обновлении или замене образов) существующих баз их следует загрузить, нажав на «*». После нажатия появится предупреждающее сообщение, представленное на рисунке 3.11.

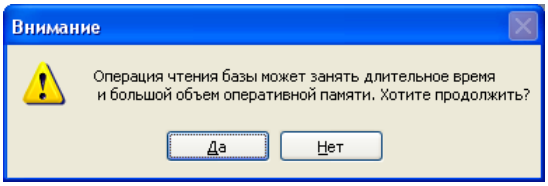

Рисунок 3.11 – Предупреждающее сообщение

Чтение большой базы требует значительного времени и ресурсов ПЭВМ, поэтому операцию можно отменить, нажав «Нет». При нажатии «Да» запуститься процедура загрузки базы.

После окончания загрузки дерево каталогов заполнится ранее созданными базами пользователей и содержащимися в них записями (образы). Для просмотра образа отпечатка пальца следует выбрать каталог пользователя и соответствующий подкаталог пальца руки, как показано на рисунке 3.12.

При нажатии «Ввести набор отп.». запустится процедура захвата набора образов выбранного пальца.

Для замены образа отпечатка пальца следует выбрать в дереве каталогов необходимый палец и нажать «Заменить отп.» После чего запуститься процедура захвата соответствующего образа.

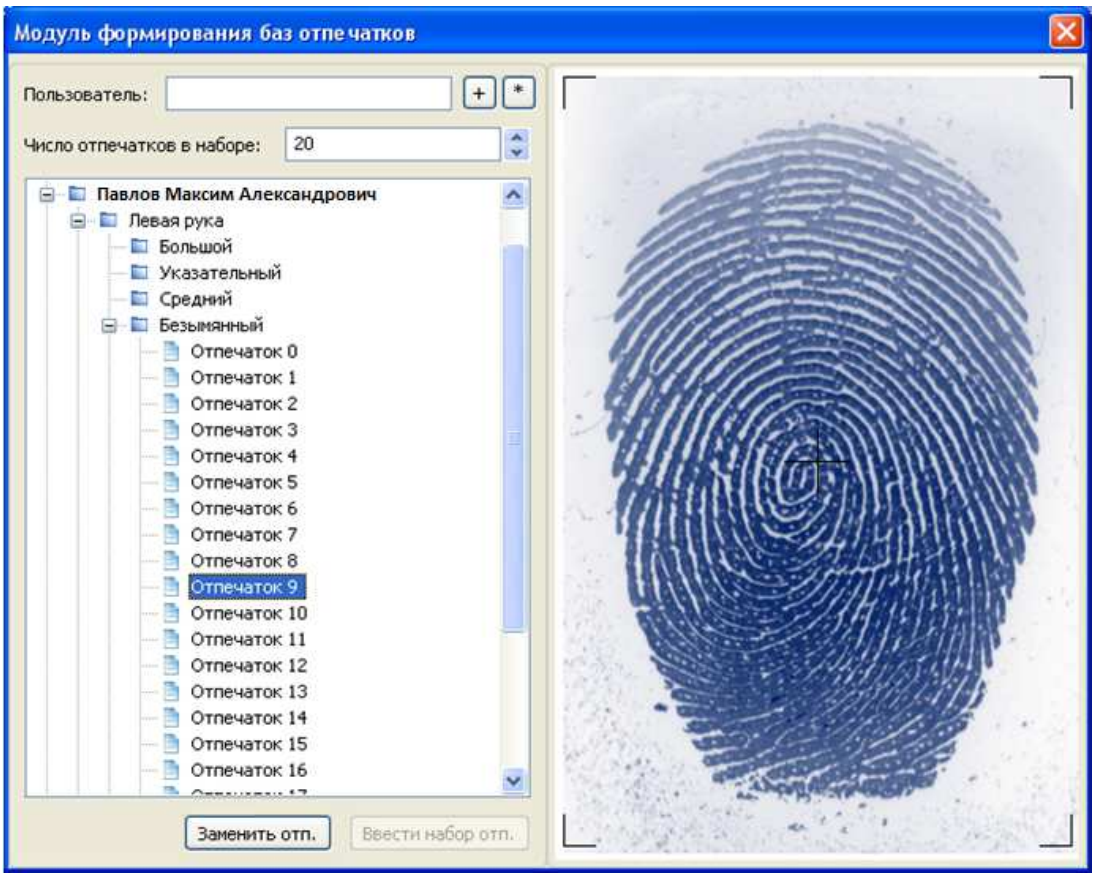

Рисунок 3.12 – Просмотр образа отпечатка пальца

3.2 Построение баз данных «Свой» и «Чужой»

Для моделирования нейросетевых преобразователей и нечетких экстракторов, преобразующих биометрические данные в код доступа, требуется экспериментальная база - биометрические образы. В рамках дипломного проекта разрабатываются способы обезличивания ПДН с использованием нечетких экстракторов и нейросетевых преобразователей, которые используют биометрические данные отпечатков пальцев людей для преобразования в код доступа с целью последующей аутентификации. Следовательно, необходимо сформировать базу отпечатков пальцев реальных людей. Разработанные модели нечеткого экстрактора и нейросетевого преобразователя предполагают, что для расчета избыточности корректирующего кода необходимо знать распределение биометрических параметров двух множеств – образа «Свой» и образа «Чужой». Образ «Свой» должен реально отражать распределение биометрических параметров

легитимного пользователя, который предъявляет системе аутентификации отпечаток пальца. Образ «Чужой» должен реально отражать распределение биометрических параметров несанкционированного пользователя (злоумышленника), который пытается подобрать отпечаток пальца легитимного пользователя.

Для формирования базы образов была использована программная среда сбора отпечатков пальцев и сканер отпечатков пальцев. Базу отпечатков пальцев «Свой» было решено составить из 100 образов отпечатков пальцев по 20 примеров. В программной среде сбора отпечатков пальцев, с помощью сканера отпечатков пальцев осуществлен ввод 20 примеров каждого из 100 отпечатков пальцев. Наличие большого количества примеров в выборке позволит ее разбить на обучающую и тестовую, что потребуется при сравнении качества принимаемых решений нечетким экстрактором и нейросетевым преобразователем биометрия-код.

В программной среде сбора отпечатков пальцев также была сформирована база данный «Чужой» из 100 различных отпечатков пальцев.

3.3 Моделирование нейросетевого преобразователя биометрия-код и нечеткого экстрактора

Моделирование преобразователя биометрия-код и нечеткого экстрактора проводилось с помощью программы автоматизации статистических расчетов. В качестве базы отпечатков пальцев образов «Свой» использовалось 5 пальцев руки. В программной среде сбора отпечатков пальцев с помощью сканера отпечатков пальцев был осуществлен ввод 100 образов по 20 примеров. При моделировании база примеров была разделена на обучающую выборку *svTable* и тестовую выборку *testTable*. Обучающая выборка использовалась для определения маски и эталонного биометрического кода для биометрического образа «Свой». А тестовая – для вычисления избыточности корректирующего кода БЧХ. После

дискретизации непрерывных биометрических параметров получены три таблицы (базы) *svDTable*, *testDTable* и *chDTable*.

При моделировании нечеткого экстрактора параметр *threshold* (вероятность ошибки первого рода) функций *funcFindMask (svDTable, threshold)* и *funcEtalonKey (svDTable, threshold)* принимал значения от 0,1 до 0,01 с шагом 0,01.

Для каждой выборки *svDTable*, *testDTable*, *chDTable* получено распределения расстояний Хэмминга *svHemming*, *testHemming*, *chHemming* соответственно.

При моделировании нечеткого экстрактора процент ошибок в эталонном биометрическом коде образа «Свой» рассчитывался как отношение *max(testHemming)* и *rows(etalonKey)*, результат которого используется в качестве входного параметра функции *funcExcess (errPer)*.

При моделировании нечеткого экстрактора длина кода доступа, формируемого нечетким экстрактором, вычислялась как отношение *rows(etalonKey)* и *funcExcess (errPer)*. Затем определялось целая часть значения кода доступа с помощью стандартной функции Mathcad *trunc (rows(etalonKey) / funcExcess(errPer))*.

Для каждого эталонного биометрического кода образа «Свой» рассчитывалась вероятность ошибки второго рода, то есть вероятность пропуска системой биометрической аутентификации на основе нечеткого экстрактора «Чужого». Ошибка рассчитывалась как интеграл от стандартной функция Mathcad *dnorm (x, mu, sigma)*, которая возвращает плотность вероятности нормального распределения со средним *mu* и среднеквадратическим отклонением *sigma*:

$$P_{II} = \int_{-\infty}^{\max(testHemming)} dnorm(x, mean(chHemming), stdev(chHemming))\, dx, \quad (3.1)$$

где:

– *mean*(*chHemming*) – стандартная функция Mathcad для вычисления математического ожидания;

– *stdev*(*chHemming*)) – стандартная функция Mathcad для вычисления среднеквадратического отклонения;

– x – непрерывная переменная.

Текст программы для статистической оценки нейросетевых преобразователей и нечетких экстракторов представлен в приложении А.

Результаты моделирования нечеткого экстрактора и нейросетевого преобразователя представлены в приложении Б.

На рисунке 3.13 показано распределение значений расстояний Хэмминга между биометрическими кодами длиной 66 бит.

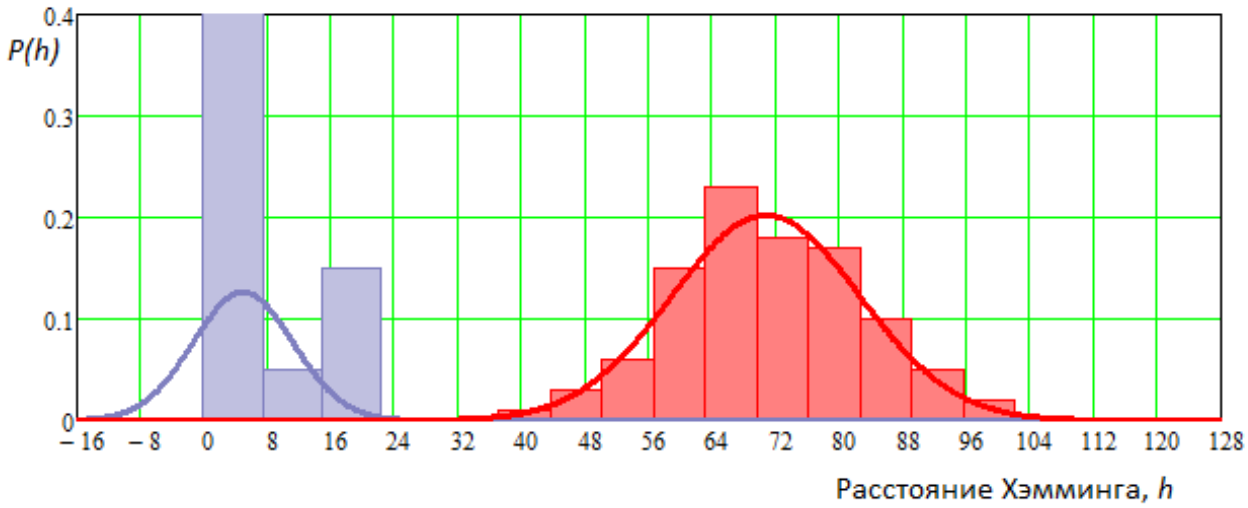

Рисунок 3.13 – Распределение значений расстояний Хэмминга между биометрическими кодами нечеткого экстрактора

Максимальное число ошибок, возникающих в эталонном биометрическом коде равно 6, что составляет 9%. Это позволяет использовать в системе аутентификации код доступа длиной всего 13 бит.

По формуле (3.1) величина:

$$P_{II} \approx 3 \times 10^{-3}. \qquad (3.2)$$

Стойкость преобразователя биометрия-код на основе нечеткого экстрактора к атакам подбора определяется как обратная величина от P_{II}:

$$D = \frac{1}{P_{II}} = \frac{1}{3 \times 10^{-3}} = 333{,}3\,. \tag{3.3}$$

Результаты моделирования нечеткого экстрактора и нейросетевого преобразователя представлены в приложении А.

Моделирование нейросетевого преобразователя биометрия-код проводилось с использованием алгоритма автоматического обучения по ГОСТ Р 52633.5–2011 [16] и для этого были сформированы выборки двух классов образов – «Чужой» и «Свой», представленные в виде векторов непрерывных биометрических параметров.

Преобразователь биометрия-код был реализован как однослойная ИНС с m входами и n выходами, описываемая следующей формулой:

$$key_i = \varphi\left(\sum_{j=1}^{m} w_{i,j} \cdot v_j + b_i\right) \tag{3.4}$$

где:

- key_i – разряд выходного кода;
- v_j – непрерывный биометрический параметр;
- $w_{i,j}$ – весовые коэффициенты *i*-го нейрона;
- b_i – смещение;
- φ – нелинейная (пороговая передаточная) функция;
- m – число параметров вектора биометрических параметров (входов ИНС);
- n – число разрядов выходного кода (число нейронов, выходов ИНС).

Нелинейная функция φ от суммы s (линейной комбинации входных биометрических параметров) выглядит так:

$$\varphi(s)=\begin{cases}1 & s\geq 0\\ 0 & s<0\end{cases} \qquad (3.5)$$

Обучение ИНС проходило на двоичных разрядах кода длиной 256 бит, который генерировался случайно. Расчет весовых коэффициентов $w_{i,j}$ нейронов осуществлялся пропорционально качеству биометрических параметров.

При обучении каждого нейрона на биометрических параметрах образа «Свой» необходимо исходить из условия равной вероятности состояний «0» и «1» для биометрических параметров образа «Чужой», как показано на рисунке 3.14.

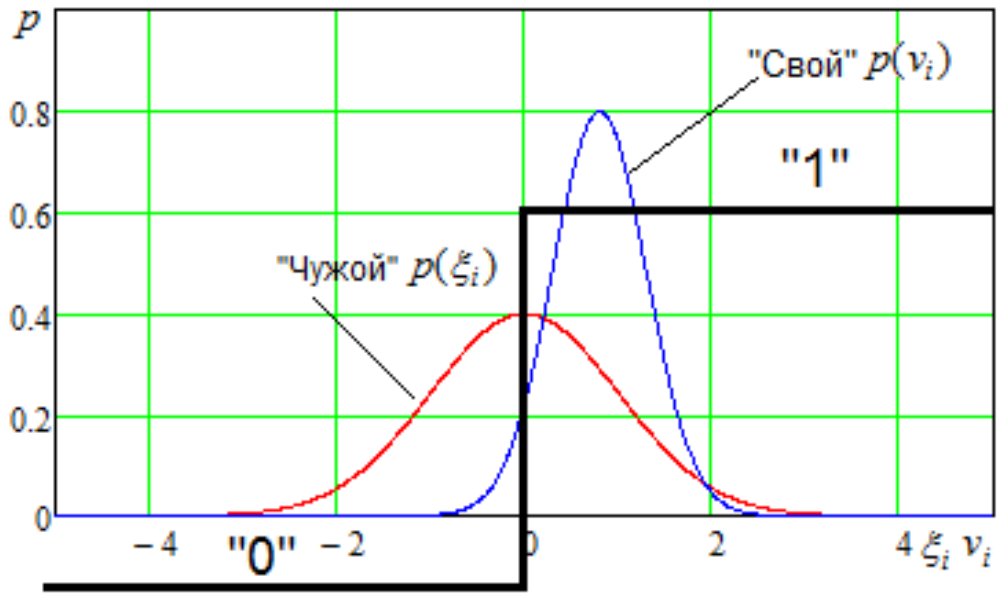

Рисунок 3.14 – Равновероятные значения «0» и «1»

Как видно из рисунка, распределение значений i- го биометрического параметра $p(\xi_i)$ образа «Чужой» имеет математическое ожидание равное 0, поэтому если на выходе нейрона требуется состояние «0», то знак весового коэффициента при обучении необходимо изменить на противоположный.

Качество работы нейросетевого преобразователя биометрия-код оценивалось как обобщающая способность обученной ИНС. То есть возможность получения точного значения кода key на выходе ИНС при

подаче на ее вход тестовой выборки, содержащей разные примеры одного и того же рукописного слова.

Для вычисления вероятности ошибок второго рода P_{II} на вход ИНС последовательно подавалось 100 разных отпечатков пальцев. На выходе полученные кодовые отклики ИНС один за другим сравнивались с кодом «Свой» в метрике Хэмминга. Сравнение кодов дает распределение значений расстояний Хэмминга, которое показано на рисунке 3.15.

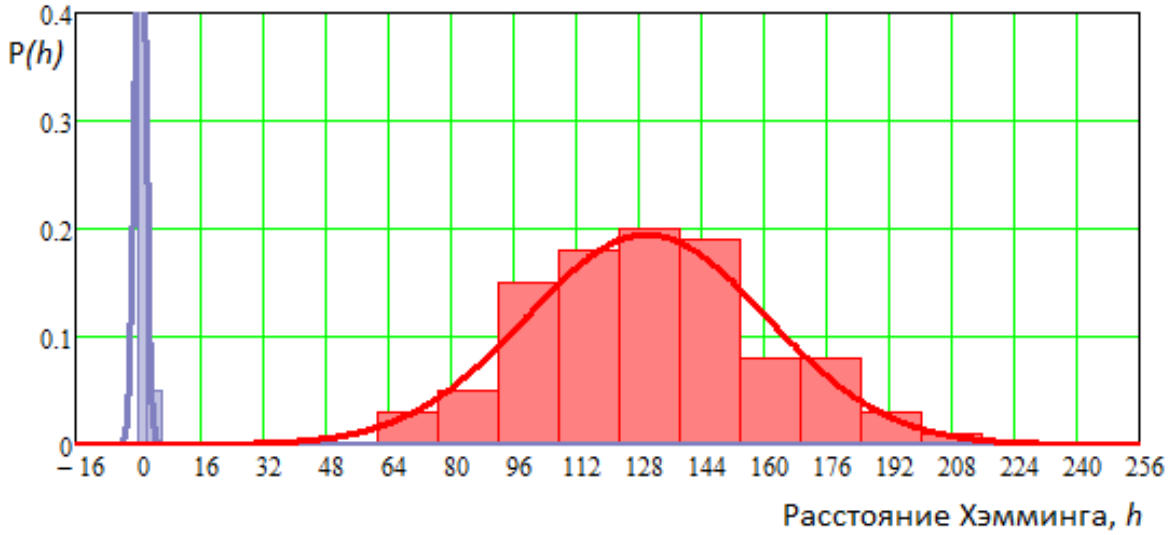

Рисунок 3.15 – Распределение значений расстояний Хэмминга между биометрическими кодами нейросетевого преобразователя

Как видно из рисунка, минимальным расстоянием оказалось h_{min} равно 64. Для численной оценки P_{II} нейросетевого преобразователя биометрия-код с разрядностью выходного кода $m > 32$ в стандарте ГОСТ Р 52633.3–2011 [14] рекомендовано использовать функцию нормального закона распределения:

$$P_{II} \approx \frac{1}{2} - \frac{1}{\sqrt{2\pi}} \cdot \int_{0}^{E(h)/\sigma(h)} \exp(-t^2/2)dt, \qquad (3.6)$$

где:

- $E(h)$ – математическое ожидание распределения значений расстояний Хэмминга;
- $\sigma(h)$ – среднеквадратическое отклонение распределения значений расстояний Хэмминга;
- t – непрерывная переменная.

Величина P_{II} приблизительно равно 0,0025. Стойкость нейросетевого преобразования «биометрия-код» к атакам подбора определяется как обратная величина от P_{II}:

$$D = \frac{1}{P_{II}} = \frac{1}{0{,}0025} \approx 400 . \quad (3.7)$$

3.4 Статистическая оценка принимаемых решений биометрической системой

Формально ИНС описывается матрицей весовых коэффициентов, поэтому для формирования кода доступа необходимо хранить ее в памяти. В стандарте ГОСТ Р 52633.4 дано определение нейросетевого биометрического контейнера как блока данных для хранения параметров обученной ИНС.

При открытом хранении матрицы весовых коэффициентов в нейросетевом контейнере возможно проведение процедуры восстановления неизвестного биометрического образа «Свой». Процедура восстановления заключается в том, что метрика Хэмминга позволяет выделить наиболее близкие биометрические образы «Чужой» к биометрическому образу «Свой» и использовать их для создания искусственных примеров путем скрещивания согласно ГОСТ Р 52633.2-2010. Результатом скрещивания является второе поколение биометрического образа «Чужой». Таким образом, можно получить третье, четвертое, пятое поколение. По мере увеличения числа поколений расстояние Хэмминга уменьшается, как показано на рисунке 3.16.

По мере увеличения числа поколений матрица весовых коэффициентов

обращается. Тем самым удается получить до 90% биометрических параметров неизвестного биометрического образа. Недостаток, заключающийся в восстановлении биометрических параметров, имеют не только нейросетевые преобразователи с открытым хранением матрицы весовых коэффициентов в биометрическом контейнере, но и нечеткие экстракторы.

Как показано в работах биометрический контейнер может быть защищен с помощью механизма размножения ошибок. Этот механизм может быть построен на основе обратимого шифрования матрицы весовых коэффициентов. Для чего необходимо часть выходного ключа, формируемого ИНС, использовать для шифрования параметров нейронов, значения на выходе которых еще не получены.

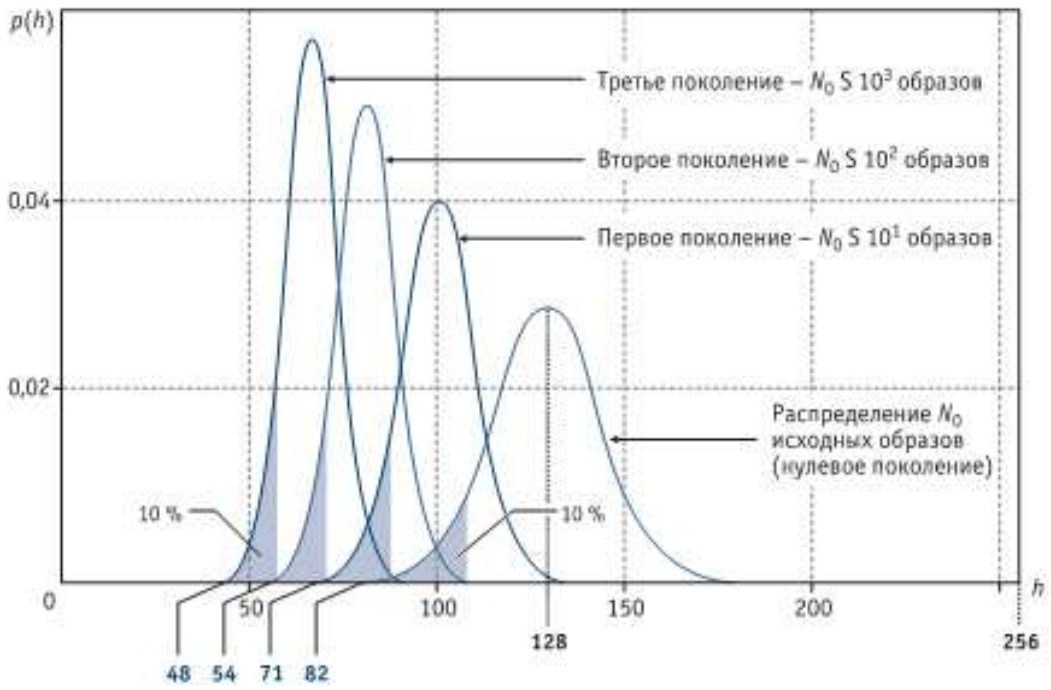

Рисунок 3.16 – Уменьшение значений расстояний Хэмминга между кодами «Свой» и «Чужой» при селекции и скрещивании

Таким образом, для биометрического образа «Свой» параметры нейронов будут последовательно расшифровываться, и на выходах ИНС сформируется точное значение ключа.

Иначе произойдет при подаче на входы ИНС значений параметров

биометрического образа «Чужой». В этом случае после первого неверно сформированного бита на выходе нейрона последующее расшифровывание параметров нейронов происходит неправильно, что приводит к хешированию параметров обученной ИНС (эффект размножения ошибок).

Эффект размножения ошибок при оценке стойкости нейросетевого преобразования биометрии в код доступа с использованием защищенного биометрического контейнера дает иное распределение значений расстояний Хэмминга. Распределение значений расстояний Хэмминга между кодовыми откликами ИНС и кодом «Свой» представлено на рисунке 3.17.

Механизм размножения ошибок не позволяет наблюдать реальное распределение значений расстояний Хэмминга. Следовательно, получение биометрических параметров неизвестного биометрического образа становится вычислительно сложной задачей.

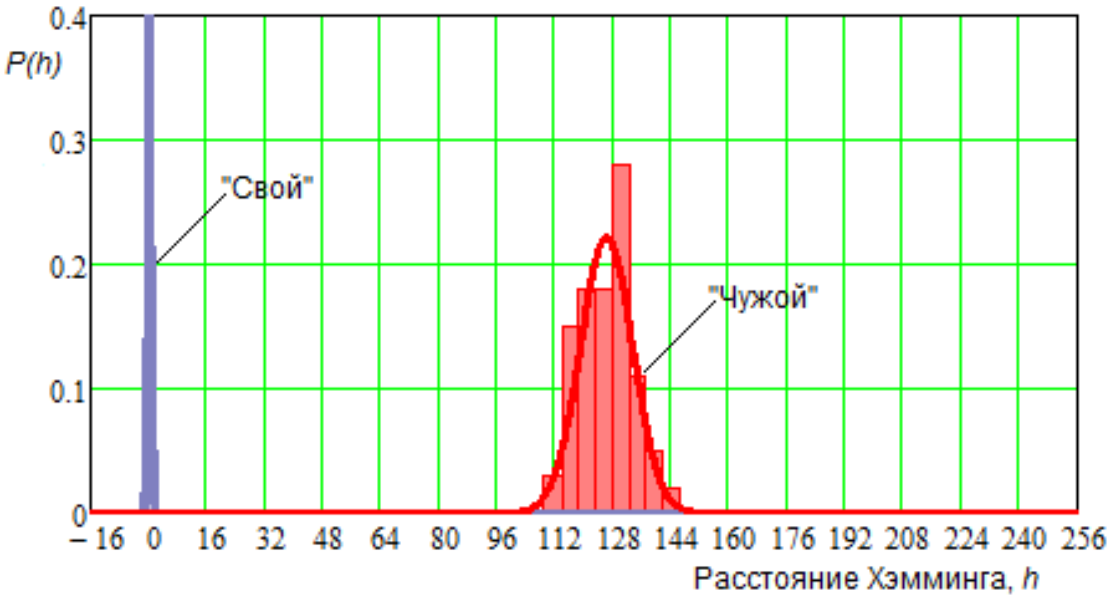

Рисунок 3.17 – Распределение значений расстояний Хэмминга между кодовыми откликами ИНС и кодом «Свой»

Экспериментальные исследования показали, что преобразователи биометрия-код на основе нечетких экстракторов имеют малую длину кода доступа (16 бит и менее). Из-за неоднозначного воспроизведения биометрических данных человека необходимо исправлять более 10% ошибок

в биометрическом коде. Это приводит к высокой избыточности корректирующего кода, которая превышает 400%. Поэтому получить код произвольной длины оказывается невозможно с помощью нечеткого экстрактора. А малая длина кода создает угрозу его подбора простым перебором.

Нечеткие экстракторы не могут обеспечить тайны биометрических образов, поскольку простое гаммирование биометрического кода не защищает биометрические параметры.

Преимуществом нейросетевых преобразователей биометрия-код является возможность формирования ИНС кода доступа произвольной длины. За счет выбора кода доступа длиной 256 бит его подбор простым перебором становится вычислительно сложной операцией.

Стойкость к атакам подбора биометрических данных для нейросетевого преобразователя и нечеткого экстрактора оказывается сравнимой. Однако за счет использования механизма размножения ошибок надежность нейросетевых преобразователей повышается.

Таким образом, нейросетевые преобразователи биометрия-код целесообразнее использовать в системах биометрической аутентификации, а также при разработке безопасных протоколов биометрико-криптографической аутентификации личности.

3.5 Выводы по третьему разделу

Сформирована база «Свой» путем ввода 100 образов по 20 примеров отпечатков пальцев в программной среде сбора отпечатков пальцев.

Сформирована база «Чужой», состоящая из 100 примеров разных отпечатков пальцев.

Разработана программа моделирования и статистической оценки нейросетевых преобразователей и нечетких экстракторов.

Проведено моделирование и выполнено сравнение вероятностных характеристик нейросетевых преобразователей и нечетких экстракторов, с

применением баз данных «Свой» и «Чужой», полученных в программной среде сбора отпечатков пальцев.

В ходе моделирования установлено, что при наличии более 10% ошибок в векторе двоичных биометрических параметрах использовать нечеткий экстрактор для обезличивания биометрических данных невозможно, так как нельзя получить корректирующий код. Нейросетевые преобразователи лишены подобного недостатка, так как позволяют формировать код произвольной длины, однако их применение также затруднительно для отпечатков пальцев с низким качеством папиллярного рисунка.

ЗАКЛЮЧЕНИЕ

Подводя итоги ВКР, можно сделать вывод, что решены все поставленные задачи и достигнута цель ВКР.

Проведен анализ зарубежных и отечественных технологий преобразования биометрических данных в код аутентификации (биометрия-код), который показал, что существует два основных направления решения задачи. Первое направление характеризуется использованием нечетких экстракторов на основе кодов с обнаружением и исправлением ошибок. Второе направление характеризуется применением больших искусственных нейронных сетей. Анализ литературы показал, что исследования нечетких экстракторов проходят преимущественно за рубежом. В РФ создано и активно развивается направление нейросетевого преобразования биометрических данных человека в код доступа. Разработаны отечественные стандарты высоконадежной нейросетевой биометрической аутентификации. Тогда как нечеткие экстракторы не являются стандартизированной технологией.

Разработаны способы обезличивания персональных данных в биометрических системах. В первом способе используется нейросетевой преобразователь биометрия-код. Второй способ отличается использованием нечеткого экстрактора.

Разработана программа автоматизации статистических расчетов, проведено моделирование работы нечеткого экстрактора и нейросетевого преобразователя, в ходе которого проведена оценка основных его характеристик с использованием баз биометрических образов «Свой» и «Чужой», сформированных в программной среде сбора отпечатков пальцев.

Проведено моделирование и выполнено сравнение вероятностных характеристик нейросетевых преобразователей и нечетких экстракторов, с применением баз данных "Свой" и "Чужой", полученных в программной среде сбора отпечатков пальцев. В ходе моделирования установлено, что при

наличии более 10% ошибок в векторе двоичных биометрических параметрах использовать нечеткий экстрактор для обезличивания биометрических данных невозможно, так как нельзя получить корректирующий код. Нейросетевые преобразователи лишены подобного недостатка, так как позволяют формировать код произвольной длины, однако их применение также затруднительно для отпечатков пальцев с низким качеством папиллярного рисунка.

По результатам дипломного проекта опубликована статья на тему «Способы обезличивания персональных данных в биометрических системах» в выпуске №12 (68) журнала «Современные научные исследования и инновации», включенного в РИНЦ (ISSN 2223-4888) [26].

Техническое задание на дипломное проектирование выполнено в полном объёме.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Болл Руд и др. Руководство по биометрии. / Болл Руд, Коннел Джонатан Х., Панканти Шарат, Ратха Налини К., Сеньор Эндрю У. // Москва: Техносфера, 2007. -368 с.

2 Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. Пенза: Изд-во ПГУ, 2005. -273 с.

3 Barni M., Bianchi T., Catalano D., Raimondo M., Labati R., Failla P., Fiore D., Lazzeretti R., Piuri V., Scotti F.,Piva A. Privacy-preserving fingercode authentication // 12th ACM Workshop on Multimedia and Security Pro-ceedings, 2010. P. 231–240.

4 Bazakos M.E., Yunqian M., Johnson A.H. Fast Access Control Technology Solutions (FACTS) // Proc. of IEEE Conference on Advanced Video and Signal Based Surveillance (AVSS2005), 2005, p.312-317.

5 Clarke R. Human identification in information systems: Management challenges and public policy issues// Information Technology and People, vol. 7, no. 4, 1994, p. 6-37.

6 Spaun N., Bruegge R. Forensic Identification of People from Images and Video // 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems, 2008. BTAS 2008. p. 1-4.

7 Fairhurst M.C. Document Identity, Authentication and Ownership: The Future of Biometric Verification// ICDAR, Seventh International Conference on Document Analysis and Recognition, vol. 2, 2003, p.1108.

8 Schouten B., Jacobs B. Biometrics and their use in e-passports // Image and Vision Computing, v.27(3), February 2009, p.305-312.

9 ISO/IEC 19785 «Information Technology – Common Biometric Exchange Formats Framework»

10 ISO/IEC 19794 «Information Technology – Biometric Data Interchange Formats»

11 ГОСТ Р 52633.0-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».

12 ГОСТ Р 52633.1-2009 «Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации»

13 ГОСТ Р 52633.2-2010 «Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации»

14 ГОСТ Р 52633.3-2011 Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора.

15 ГОСТ Р 52633.4-2012 «Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия-код».

16 ГОСТ Р 52633.5-2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа».

17 ГОСТ Р ИСО/МЭК 19794-2-2006, «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2: Данные изображения отпечатка пальца - контрольные точки».

18 ГОСТ Р ИСО/МЭК 19794-8-2009, «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 8: Данные структуры остова отпечатка пальца».

19 Харитонов А.В. Обзор биометрических методов идентификации личности // NB: Кибернетика и программирование. — 2013. - № 2. - С.12-19.

20 Uludag U., Pankanti S., Prabhakar S., Jain A. K. Biometric cryptosystems: issues and challenges // Proceedings of the IEEE. 2004. Vol. 92. № 6. P. 948–960.

21 Arakala A., Jeffers J, Horadam K.J. Fuzzy Extractors for Minutiae-Based Fingerprint Authentication // Advances in Biometrics, Springer, pp. 760-769, 2007.

22 Bringer J., Despiegel V. Binary feature vector fingerprint representation frommінutiae vicinities // 4th IEEE Conference (International) on Biometrics: Theory, Applications and Systems (BTAS-10) Proceedings, 2010. P. 1–6.

23 Нейросетевая защита персональных биометрических данных. Монография / Под ред. Ю.К. Язова (редактор и автор). М.: Радиотехника, 2012.-157 с.

24 ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».

25 Dodis Y., Ostrovsky R., Reyzin L., Smith A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data // SIAM J. Computing, 2008. Vol. 38.No. 1. P. 97–139.

26 Современные научные исследования и инновации [Текст]: электронный научно-практический журнал / издатель ООО «Международный научно-инновационный центр». РИНЦ. ISSN 2223-4888. №12 (68) статья: «Способы обезличивания персональных данных в биометрических системах». [М. А. Павлов] – опубл. 2016-12-29. – М.: – 5с.

ПРИЛОЖЕНИЕ А

(обязательное)

Текст программы для

статистической оценки нейросетевых преобразователей и нечетких экстракторов

Биом. параметры обучающей выборки"Своего"

```
svTable := | for ii ∈ 0..rows(svBase) − 1
           |   point ← READPRN(svBase_ii)
           |   r ← rows(point)
           |   for i ∈ 0..r − 1
           |     svGrid1_i ← point_i
           |   svGrid ← svGrid1  if ii = 0
           |   svGrid ← augment(svGrid, svGrid1)  otherwise
           | svGrid
```

Нормировка базы "Свой"

$$\text{funcTableNorm}(\text{Table}) := \left| \begin{array}{l} \text{for } i \in 0..\text{cols}(\text{Table}) - 1 \\ \quad \text{for } j \in 0..\text{rows}(\text{Table}) - 1 \\ \quad\quad \text{TableNorm}_{j,i} \leftarrow \dfrac{\text{Table}_{j,i} - \text{chAver}_j}{\sqrt{\text{chDisp}_j}} \\ \text{TableNorm} \end{array} \right.$$

Нормировка тестового образа

$$\text{funcNorm}(\text{coeffs}) := \left| \begin{array}{l} \text{for } j \in 0..\text{rows}(\text{coeffs}) - 1 \\ \quad \text{normCoeffs}_j \leftarrow \dfrac{\text{coeffs}_j - \text{chAver}_j}{\sqrt{\text{chDisp}_j}} \\ \text{normCoeffs} \end{array} \right.$$

Расчет качества

$$\text{funcKach1}(\text{svAver}, \text{svDisp}) := \left| \begin{array}{l} \text{for } i \in 0..\text{rows}(\text{svAver}) - 1 \\ \quad \text{Kach}_i \leftarrow \dfrac{\lvert \text{svAver}_i \rvert}{\sqrt{\text{svDisp}_i}} \quad \text{if } \text{svDisp}_i > 0.01 \\ \quad \text{Kach}_i \leftarrow 0 \quad \text{otherwise} \\ \text{Kach} \end{array} \right.$$

Случайная генерируемая таблица связей

```
funcTableSvjaz(nNeuron, Inputs, numberParam) :=
    for i ∈ 0.. nNeuron − 1
      for j ∈ 0.. Inputs − 1
        Net_{i,j} ← 0
    for i ∈ 0.. nNeuron − 1
      for j ∈ 0.. Inputs − 1
        Usl ← 0
        Kol ← 0
        while Usl = 0
          RandomInteger ← trunc(rnd(numberParam − 1))
          for jj ∈ 0.. Inputs − 1
            if RandomInteger = Net_{i,jj}
              Kol ← Kol + 1
              break
          if Kol = 0
            Usl ← 1
            Net_{i,j} ← RandomInteger
          Kol ← 0
    Net
```

Подача на вход нейронной сети базы

funcSumErrorKeyNet(Table, TableSvjaz, TableVes, TableZnak, Key) :=

```
for bio ∈ 0.. cols(Table) − 1
    SumError_bio ← 0
    for i ∈ 0.. cols(Key) − 1
        Summator_i ← 0
        for j ∈ 0.. cols(TableVes) − 1
            Summator_i ← Summator_i + (Table_(TableSvjaz_(i,j), bio)) · (TableVes_(i,j)) · TableZnak_(i,j)
    for i ∈ 0.. cols(Key) − 1
        TestKey_(0,i) ← 0 if Summator_i ≤ 0
        TestKey_(0,i) ← 1 if Summator_i > 0
    for i ∈ 0.. cols(Key) − 1
        SumError_bio ← SumError_bio + 1 if TestKey_(0,i) ≠ Key_(0,i)
SumError
```

ПРИЛОЖЕНИЕ Б

(обязательное)

Результаты моделирования нечеткого экстрактора и нейросетевого преобразователя

В ходе экспериментальной проверки модели нечеткого экстрактора, преобразующего биометрические данные отпечатка пальца, определены основные ее характеристики, которые представлены в таблице Б.1.

Таблица Б.1 – Результаты моделирования нечеткого экстрактора на базах "Свой" и "Чужой"

Палец	P_I, ошибка первого рода	n, длина вектора параметров, бит	H_{max}, макс. число ошибок	Число ошибок, %	k, длина ключа, бит	P_{II}, ошибка второго рода
Правый большой	0,1	139	41	29,496403	–	0,005
	0,09	120	27	22,5	–	0,004
	0,08	120	27	22,5	–	0,004
	0,07	120	27	22,5	–	0,004
	0,06	120	27	22,5	–	0,004
	0,05	66	6	9,0909091	13	0,003
	0,04	66	6	9,0909091	13	0,003
	0,03	66	6	9,0909091	13	0,003
	0,02	66	6	9,0909091	13	0,003
	0,01	66	6	9,0909091	13	0,003
Правый указательный	0,1	151	45	29,801325	–	0,005
	0,09	151	45	29,801325	–	0,005
	0,08	151	45	29,801325	–	0,005
	0,07	151	45	29,801325	–	0,005
	0,06	151	45	29,801325	–	0,005
	0,05	73	7	9,5890411	14	0,003
	0,04	73	7	9,5890411	14	0,003
	0,03	73	7	9,5890411	14	0,003
	0,02	73	7	9,5890411	14	0,003
	0,01	73	7	9,5890411	14	0,003
Правый средний	0,1	175	23	13,142857	–	0,004
	0,09	151	19	12,582781	–	0,004
	0,08	151	19	12,582781	–	0,004
	0,07	151	19	12,582781	–	0,004
	0,06	151	19	12,582781	–	0,004
	0,05	103	8	7,7669903	34	0,003
	0,04	103	8	7,7669903	34	0,003
	0,03	103	8	7,7669903	34	0,003
	0,02	103	8	7,7669903	34	0,003
	0,01	103	8	7,7669903	34	0,003

Продолжение таблицы Б.1

Палец	$P_{I,}$ ошибка первого рода	n, длина вектора параметров, бит	H_{max}, макс. число ошибок	Число ошибок, %	k, длина ключа, бит	$P_{II,}$ ошибка второго рода
Правый безымянный	0,1	138	39	28,26087	–	0,004
	0,09	121	24	19,834711	–	0,004
	0,08	121	24	19,834711	–	0,004
	0,07	121	24	19,834711	–	0,004
	0,06	121	24	19,834711	–	0,004
	0,05	68	6	8,8235294	13	0,002
	0,04	68	6	8,8235294	13	0,002
	0,03	68	6	8,8235294	13	0,002
	0,02	68	6	8,8235294	13	0,002
	0,01	68	6	8,8235294	13	0,002
Правый мизинец	0,1	137	37	27,007299	–	0,003
	0,09	123	23	18,699187	–	0,003
	0,08	123	23	18,699187	–	0,003
	0,07	123	23	18,699187	–	0,003
	0,06	123	23	18,699187	–	0,003
	0,05	57	5	8,7719298	11	0,002
	0,04	57	5	8,7719298	11	0,002
	0,03	57	5	8,7719298	11	0,002
	0,02	57	5	8,7719298	11	0,002
	0,01	57	5	8,7719298	11	0,002

В качестве экспериментальных баз использованы база биометрических образов «Свой» из 100 образов по 20 примеров отпечатков пальцев, а также база данных «Чужой» из 100 примеров разных отпечатков пальцев для оценки стойкости нечеткого экстрактора к атакам подбора выходного кода доступа.

Для сравнения качества принимаемых решений нейросетевым преобразователем с решениями, принимаемыми нечетким экстрактором на одинаковых биометрических данных получены характеристики нейронной сети, представленные в таблице Б.2.

Таблица Б.2 – Характеристики нейросетевого преобразователя на базах "Свой" и "Чужой"

Палец	k, длина ключа, бит	Ошибка первого рода P_I	Ошибка второго рода P_{II}
Правый большой	256	0,25	0,003
Правый указательный	256	0,25	0,003
Правый средний	256	0,1	0,002
Правый безымянный	256	0,1	0,003
Правый мизинец	256	0,1	0,003

Неоднозначность воспроизведения биометрических параметров человека приводит к тому, что необходимо исправлять много ошибок в биометрическом коде. Из таблицы Б.1 видно, что для некоторых биометрических образов число ошибок в биометрическом коде оказалось более 10%. Из таблицы Б.1 также видно, что для нечеткого экстрактора требуется высокая избыточность корректирующего кода – более 400%. Следовательно, получить на выходе нечеткого экстрактора код, стойкий к подбору простым перебором, оказывается невозможно.

За счет выбора кода доступа длиной 256 бит для нейросетевого преобразователя биометрия-код его подбор простым перебором становится вычислительно сложной операцией. Поэтому применение нейросетевых преобразователей в средствах биометрической аутентификации выглядит перспективнее, так как они позволяют формировать код доступа длиной 256 бит, в том числе с использованием биометрических образов, которые стабильно не воспроизводятся человеком.

ПРИЛОЖЕНИЕ В

(обязательное)

Результаты прохождения ВКР в системе «Антиплагиат»

Протокол проверки ВКР на оригинальность в системе «Антиплагиат.ВУЗ» выпускной квалификационной работы на тему «Способы обезличивания персональных дынных в биометрических системах» студента 6 курса М.А. Павлова направления подготовки 10.05.02 «Информационная безопасность телекоммуникационных систем». Специализация – разработка защищённых телекоммуникационных систем.

Скриншот отчёта о проверке ВКР в системе «Антиплагиат.ВУЗ» представлен на рисунке В1.

Руководитель ВКР: научный сотрудник лаборатории биометрических и нейросетевых технологий АО «ПНИЭИ», к.т.н. М.В. Секретов.

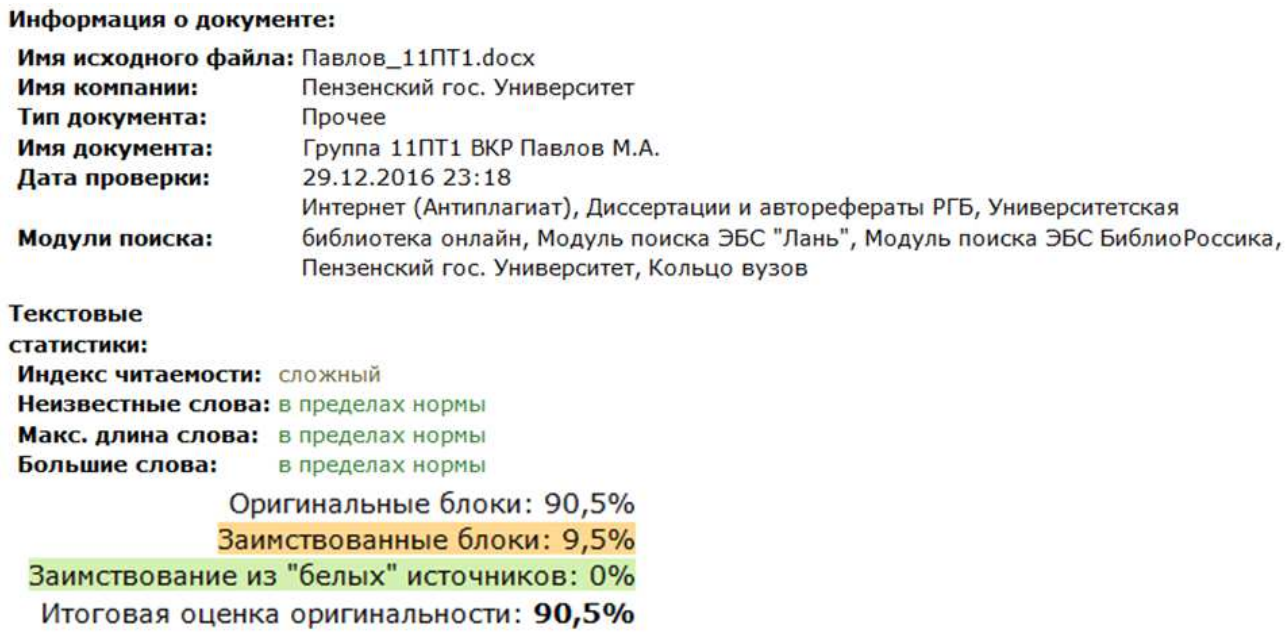

Рисунок В1 – Скриншот отчёта о проверке ВКР в системе «Антиплагиат.ВУЗ»

«___»_____ 20___г. _____М. В. Секретов