Разработка централизованной системы избирательной мультибиометрической аутентификации[1]

А.Н. Ручай, В.В. Кузнецов, А.В. Мельников, А.В. Вохминцев

Аннотация. Целью исследования является разработка централизованной системы разграничения прав доступа на основе избирательной мультибиометрической аутентификации. Новизна подхода заключается в разработке комбинированных принципов избирательности мультибиометрической аутентификации, так как на данный момент не существует подобных разработок в предложенной постановке проблемы. В зависимости от разных условий и факторов, в частности от надежности и безопасности, доступности электронных средств, удобства, стойкости к атакам и уязвимостям, болезней или увечий пользователей, может быть выбрана биометрическая аутентификация на основе комплекса биометрических характеристик: ритм ввода пароля, голос, динамика подписи и графический пароль. В работе приведены результаты разработки программного обеспечения на основе нового комбинированного подхода, кроме того, описывается архитектура системы и протоколы взаимодействия. Проведен анализ возможных атак на разработанную систему, сделаны выводы и предложены рекомендации по методам защиты от них.

Ключевые слова: мультибиометрика, мультибиометрическая аутентификация, разграничение прав доступа.

Введение

Разработчики и исследователи биометрических систем предлагают программные реализации на основе, как правило, одной биометрической характеристики без дополнительных инструментов и модулей, что создает проблемы при их использовании и эксплуатации [1, 2]. Однако современные тенденции показывают стремление использовать другой подход - создание мультибиометрических систем аутентификации личности [1, 3, 4]. Главным достоинством этого подхода является то, что безопасность доступа к защищенным ресурсам и информации может быть улучшена.

Под мультибиометрической системой будем понимать систему с использованием нескольких биометрических характеристик человека, которые могут быть интегрированы на разных уровнях и использованы различными способами [1, 5]. В мультибиометрических системах биометрические характеристики человека обрабатываются с помощью различных методов, и принятие решение происходит по объединенному решающему правилу для повышения надежности, кроме этого могут использоваться другие методы аутентификации, например, PIN–код, пароль, ритм ввода пароля, токены [6].

Мультибиометрические системы, как известно, обладают повышенной безопасностью,

[1] Исследование выполнено за счет гранта Российского научного фонда (проект №15-19-10010) и гранта Министерства образования и науки Российской Федерации (проект 2.1766.2014К).

защитой от атаки на устройство ввода (сенсор) и высокой надежностью [1]. Мультибиометрические системы могут использовать несколько биометрических характеристик, несколько биометрических образцов, несколько решающих правил, несколько схем нормализации, или методов параметризации, с помощью чего добиваются усиления надежности. Тем не менее, безопасность и надежность предлагаемых мультибиометрических систем часто приводит к дополнительным вычислительным требованиям и пользовательским неудобствам, которые могут включать в себя проблемы конфиденциальности. Поэтому при разработке мультибиометрических систем необходимо находить разумный компромисс между надежностью, безопасностью, вычислительными затратами и удобством пользователей. Этот компромисс желательно решать некоторыми автоматическими или полуавтоматическими средствами, и это решение должно сводиться к динамическому управлению безопасностью и надежностью системы в целом. Однако в литературе недостаточно внимания уделено теории, архитектуре, реализации, оценки надежности и производительности мультибиометрических систем, которые динамически обеспечивают изменяющийся уровень безопасности с помощью выбора различных параметров мультибиометрической системы.

В данной статье под избирательной мультибиометрической аутентификацией будем понимать такую мультибиометрическую систему, где динамически обеспечивается изменяющийся уровень безопасности с помощью выбора различных ее параметров, в частности, выбора конкретной биометрической характеристики. Предлагаемый подход избирательности для мультибиометрической аутентификации будет подробно описан в главе 2.

В зависимости от разных условий и факторов, в частности от доступности электронных средств, от удобства, от стойкости к атакам и уязвимостям, от болезней или увечий пользователей, может быть выбрана биометрическая аутентификация на основе следующих биометрических характеристик: ритм ввода пароля, голос, динамика подписи и графический пароль. Например, если необходимо разграничить права доступа в изолированном помещении без посторонних, то может быть использована аутентификация по голосу, по ритму ввода пароля или графическому паролю. Если помещение наоборот не обладает такими условиями, то аутентификация может быть осуществлена на основе ритма ввода пароля или по динамике подписи. Для осуществления аутентификации в мобильных или сенсорных устройствах может быть выбрана аутентификация по ритму ввода пароля, по динамике подписи или графическому паролю. На пропускных пунктах возможна аутентификация по динамике подписи. В настоящее время актуальной является задача разработки универсальных модулей, реализующих разграничение прав доступа на основе мультибиометрической аутентификации [7].

Кроме того, системы разграничения доступа на основе мультибиометрической аутентификации имеют большую практическую значимость и преимущества:

- уникальность, неотъемлемость и не отчуждаемость биометрической характеристики;
- затруднения при проведении атаки подбора по биометрической характеристике;
- независимость от операционной системы и кодировок символов;
- избирательность мультибиометрической аутентификации;
- отсутствие ошибок третьего рода, когда невозможно аутентифицировать человека из-за болезней и увечий.

Целью данного проекта является разработка, исследование и реализация централизованной системы разграничения прав доступа на основе избирательной мультибиометрической аутентификации с клиент-серверной архитектурой. Для этого необходимо решить следующие задачи:

- разработка принципов построения избирательной мультибиометрической системы;
- разработка архитектуры системы;
- разработка протокола взаимодействия;
- разработка и реализация центра и модулей биометрической аутентификации;
- тестирование и оценка разработанной централизованной избирательной мультибиометрической системы.

1. Биометрическая система аутентификации

В работах [2, 7, 8] описан разработанный комплекс модулей биометрической аутентификации для разграничения прав доступа в ОС Windows XP на примере текстозависимой верификации диктора [9, 10]. Данный комплекс модулей послужил основой для разработки и реализации централизованной системы разграничения прав доступа на основе избирательной мультибиометрической аутентификации. В [11] сформулированы основные принципы и создан прототип централизованной системы разграничения прав доступа на основе избирательной мультибиометрической аутентификации.

Самым важным аспектом методологии разработки централизованной системы разграничения прав доступа на основе избирательной мультибиометрической аутентификации является требование отраслевых стандартов, в частности, серии стандартов ГОСТ Р ИСО/МЭК 19784, 19795 и 24709. Стоит отдельно отметить, что в серии российских стандартах ГОСТ Р 52633 содержатся требования к средствам высоконадежной биометрической аутентификации.

На Рис. 1 представлена общая схема биометрической системы аутентификации, где базовыми функциями являются регистрация и сравнение. В ходе регистрации сигнал, полученный при помощи биометрических сканеров или устройств ввода, преобразуется в цифровой шаблон с помощью специальных процедур параметризации. На этапе сравнения предъявляемые биометрические данные сравниваются с шаблоном регистрации. Результатом сравнения биометрических данных является число, показывающее меру сходства.

В основу собственных разработок были положены работы [3, 4], в которых был предложен подход к созданию высокопроизводительных мультибиометрических технологий и систем на базе сервисно-ориентированной архитектуры, а также методы оптимизации и распараллеливания вычислений в задаче мультибиометрической идентификации.

С целью разработки и реализации централизованной системы разграничения прав доступа на основе избирательной мультибиометрической аутентификации были сформулированы требования к ее архитектуре [3]:

- возможность интеграции в рамках одной системы нескольких методов биометрической аутентификации;
- возможность замены и модификации библиотек, в которых реализованы методы биометрической аутентификации;
- гибкость в конфигурировании;
- обеспечение комплексной безопасности и защиты биометрических данных;
- поддержка существующих российских стандартов в сфере биометрических технологий.

Современные разработки [3] изначально учитывают масштабируемость и распределенность архитектуры биометрической системы, в рамках которой используют концепцию сервисо-ориентированной архитектуры. Для такой архитектуры принято разделять внутреннюю логику биометрических приложений на элементарные сервисы [3]:

- вычислительные сервисы, отвечающие за выполнение функций биометрических библиотек, ядро системы;
- сервисы бизнес-логики приложения;
- сервисы хранилища;
- клиентские приложения, «тонкий» клиент терминальных станций;
- вспомогательные сервисы управления, мониторинга, диагностики;

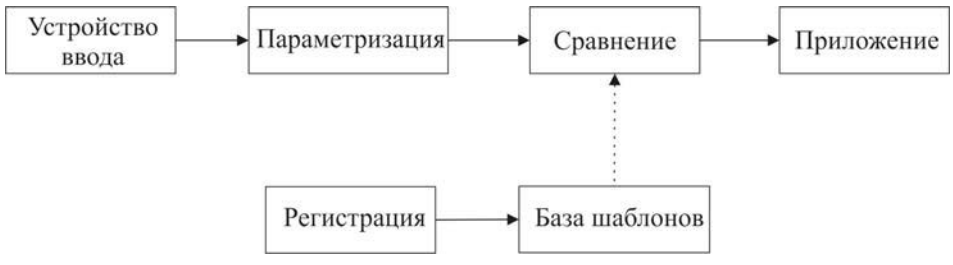

Рис. 1. Программная архитектура

• сервисы сообщений/предоставления интерфейса, отвечающие за обмен информацией между узлами системы;

• сервисы операционной системы, распределенная среда исполнения.

2. Избирательная мультибиометрическая система аутентификации

Мультибиометрия может быть использована для решения различных аспектов проблем управления безопасностью, ее главной задачей является повышение безопасности системы в целом.

Существуют различные подходы к созданию мультибиометрических систем [12, 13]. Можно выделить четыре основных метода слияния: на уровне сырых данных, на уровне шаблона, на уровне сравнения, на уровне принятия решения. Универсальная система должна учитывать всевозможные подходы к реализации мультибиометрики с помощью слияния.

Мультибиометрические системы должны быть весьма гибкими, чтобы учитывать различные требования и ограничения пользователей. Система должна быть разработана таким образом, чтобы решать проблему отсутствия конкретной биометрической характеристики (например, в результате плохого качества или физических проблем) с помощью предоставления другой доступной биометрической характеристики. Кроме этого условия, важно соблюдать требование необходимого уровня безопасности. Для этого требуется разработка динамического выбора различных правил и методов слияния в мультибиометрической системе.

Один из самых простых подходов был описан в работе [14], где были проведены эксперименты с несколькими простыми методами слияния мультибиометрических данных.

Авторы в статье [15] предложили другой интересный подход, который включает в себя проведение непрерывной аутентификации. Этот подход требует продолжительного физического присутствия пользователя и, следовательно, не подходит для некоторых типов приложений.

В работе [16] предлагается использовать несколько уровней безопасности для мультибиометрической аутентификации с тремя биометрическими характеристиками (лицо, движения губ, голос). Когда необходимый уровень безопасности низкий, то достаточно принять решение на основе двух из трех биометрических характеристик. С другой стороны, для приложений с высоким уровнем безопасности, эта система требует использования все три биометрические характеристики. Тем не менее, эта система не обеспечивает динамический способ изменения уровня безопасности. Вместо этого, администратор сам принимает решение о стратегиях и методах слияния.

Интересная архитектура для динамического управления безопасностью с участием нескольких биометрических характеристик предложена в работе [17]. Эта работа предполагает сценарий обеспечения разграничения прав доступа в здании, которое разделено на различные зоны (это могут быть разные этажи или номера комнат), и права доступа для каждого из пользователей определены соответственно для каждой из этих зон. Решения доступа в конкретной зоне могут также зависеть от решений уже принятых в других зонах. Кроме того, количество биометрических характеристик необходимых в каждой зоне и различные стратегии выбора метода слияния могут варьироваться.

Другой аспект разработки избирательной мультибиометрической системы заключается в обеспечении желаемой производительности, а также в выполнении предпочтений пользователей, ограничений пользователей, удобства пользователей и их возрастных изменений [18]. Научно-исследовательские проблемы для таких задач связаны с динамическим выбором методов слияния.

Уровень безопасности мультибиометрической системы также должен быть установлен в зависимости от предполагаемых угроз. В зависимости от предполагаемой угрозы или риска атаки эта система предписывает выбор соответствующих методов слияния.

В данной работе, в отличие от всех предыдущих работ, предлагается комбинированный подход к разработке избирательной мультибиометрической системы аутентификации, в котором используются все вышеперечисленные критерии выбора метода слияния мультибиометрических характеристик.

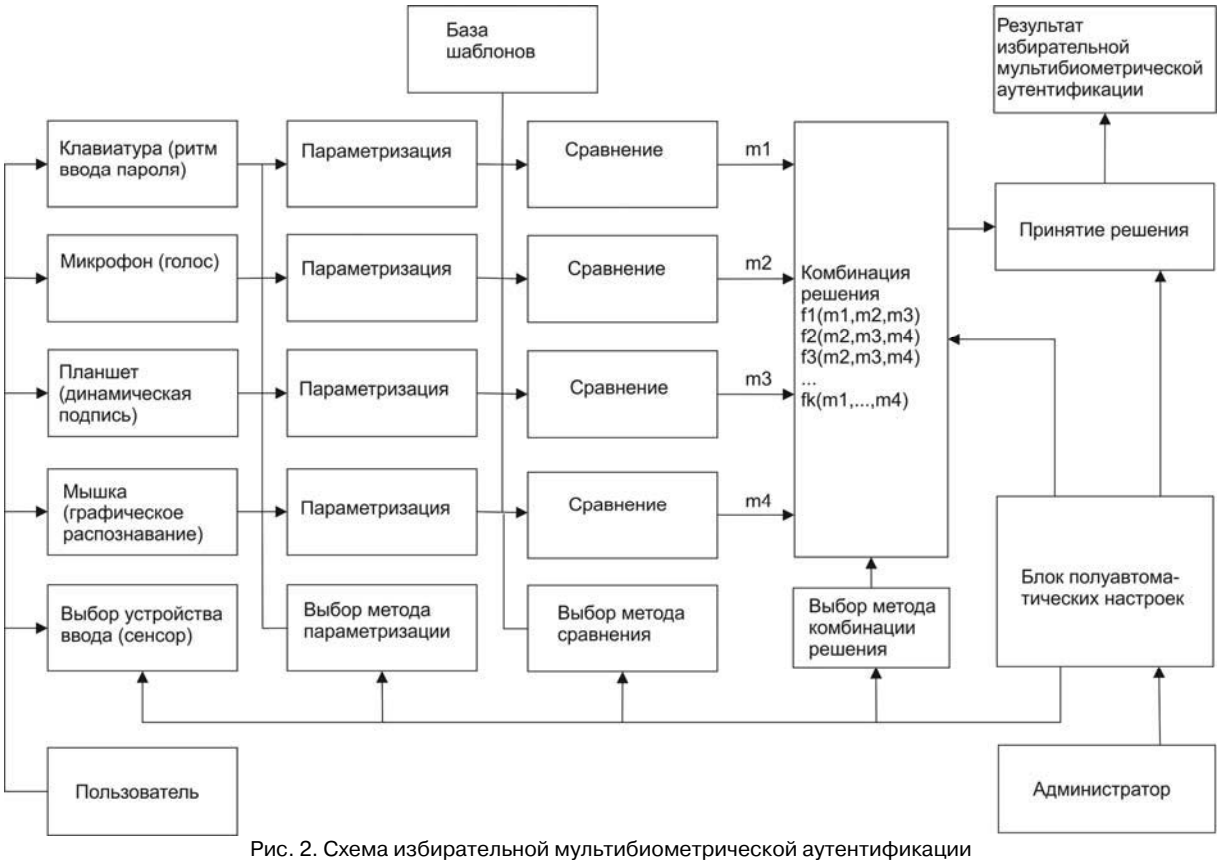

Рис. 2. Схема избирательной мультибиометрической аутентификации

Для упрощения описания критериев избирательной мультибиометрической аутентификации приведем схему на Рис. 2, где показаны основные этапы избирательной мультибиометрической аутентификации на примере ритма ввода пароля, голоса, динамика подписи и графического пароля. Данный подход и схема могут быть обобщены для любых биометрических характеристик.

Самым важным блоком в данной схеме является блок полуавтоматических настроек, который выполняет перевод всех настроек и параметров, заданных администратором и пользователем на этапе обучения. В качестве параметров выступает полуавтоматический выбор: последовательности предоставления биометрической характеристики, сам набор биометрических характеристик, устройства ввода (сенсора), метода параметризации, метода сравнения, метода комбинации решения. Под полуавтоматическим выбором понимается выбор метода слияния в виде заранее заданных жестких правил и критериев.

Перечислим базовые критерии и правила:

1. Наличие необходимых устройств ввода (сенсоров).
2. Уровень безопасности (количество необходимых биометрических характеристик).
3. Выбор очередности предоставления биометрических характеристик.
4. Результат предыдущих попыток аутентификации.
5. Особенности данной зоны (комнаты, устройств).
6. Особенности пользователей и их предпочтения, возрастные ограничения.
7. Время прохождения аутентифкации.
8. Степень угроз и вероятности атак на устройства ввода (сенсор).
9. Качество предоставляемых биометрических образцов.

Блок полуавтоматических настроек после задания всех настроек и параметров полуавтоматическим способ может выбрать необходимую решающую функцию в блоке комбинация решения f1(m1,m2,m3), …, fk(m1,…,m4), где m1, m2,

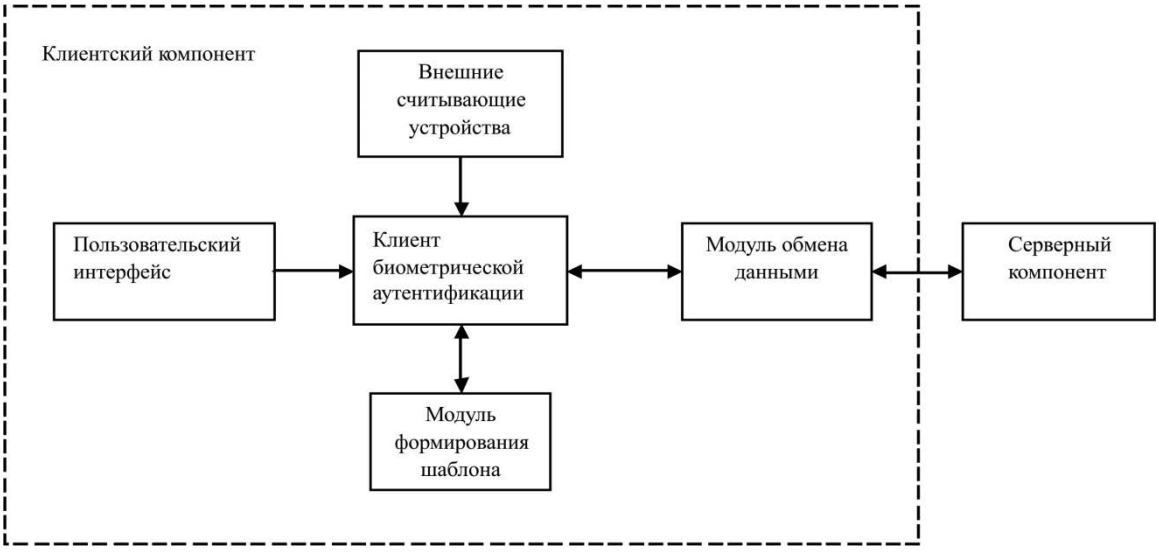

Рис. 3. Клиентский компонент архитектуры системы

m3, m4 – результат сравнения каждой биометрической характеристики в отдельности, и выбрать необходимый порог принятия решения.

Однако данная избирательная мультибиометрическая система не подбирает параметры для гарантирования определенного уровня безопасности автоматически, это является направлением дальнейших исследований и разработок.

3. Архитектура системы

На основе анализа модели существующих атак и защиты мультибиометрических систем можно сделать вывод, что многие проблемы и атаки предотвращаются с помощью цифрового кодирования, временных меток и шифрования открытого канала передачи данных [19, 20]. В связи с этим система разграничения прав доступа должна быть реализована с клиент-серверной архитектурой, что дает следующие преимущества:

- повышается общая безопасность системы;
- один мощный сервер сможет одновременно обслуживать множество клиентов;
- обеспечивается минимальная нагрузка на компьютер клиента;
- сводится к минимуму количество клиентских настроек;
- сервер можно использовать под любую ОС, а клиентские части останутся неизменными;
- клиентскую часть также можно написать под другую ОС, а сервер останется неизменным.

Клиент-серверная архитектура кроме этого позволяет отделить работу с внешними устройствами, чей интерфейс зачастую не стандартизирован, от основного вычислительного узла, который, в свою очередь, должен быть реализован с учетом требований российских и международных стандартов. На Рис. 3 и Рис. 4 изображены схемы клиент-серверной архитектуры централизованной системы разграничения прав доступа на основе избирательной мультибиометрической аутентификации.

4. Протоколы взаимодействия

Основой для протокола передачи исходных биометрических данных являются серии стандартов по обмену биометрической информации: ГОСТ Р ИСО/МЭК 19784, 19795, 24709, ГОСТ Р 52633, ИСО/МЭК ТО 24722, ИСО/МЭК 19794, 19785, 24708.

В работе рассмотрены важные аспекты разработки протокола передачи биометрических данных и успешно реализованы протоколы взаимодействия.

4.1 Формат обмена данными

Самым важным аспектом методологии разработки централизованной системы разграничения прав доступа на основе избирательной мультибиометрической аутентификации является требование отраслевых стандартов.

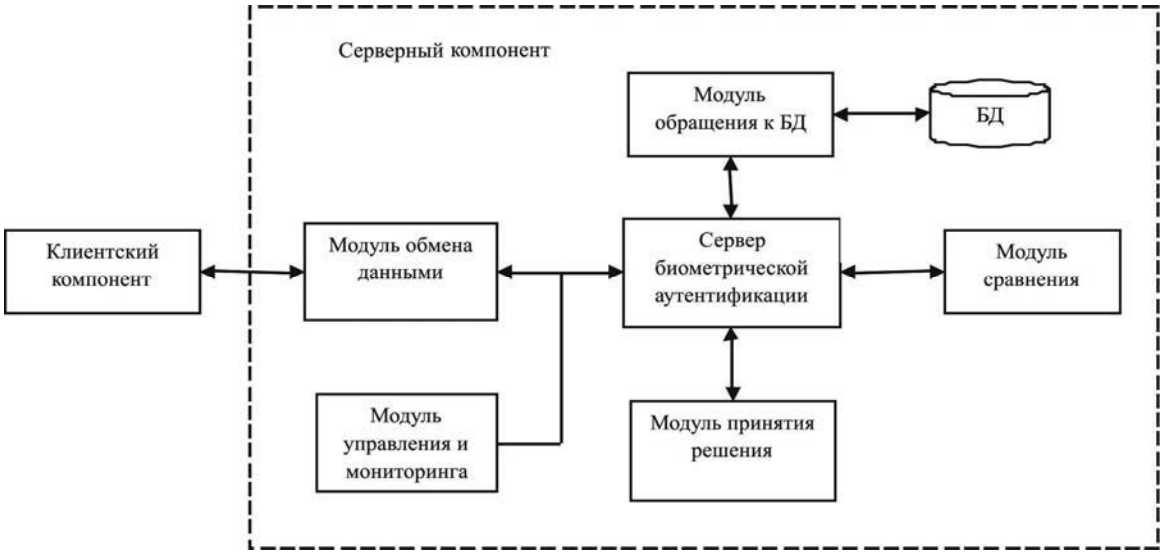

Рис. 4. Серверный компонент архитектуры системы

Согласно российским стандартам по биометрии реализация биометрической системы предполагает использование трех типов данных: исходные данные (исходные образцы), полученные с внешнего считывающего устройства (устройства ввода); данные (образцы), обработанные функциями специализированных библиотек (фильтрация, шумоочистка и т.д.); цифровой шаблон биометрического образца (набор признаков). Для передачи исходных данных, признаков и шаблонов определены две концепции биометрических интерфейсов: блок биометрических данных и запись биометрической информации.

Блок биометрических данных представляет собой формат стандартизированных данных в виде образцов и наборов признаков (шаблонов) в соответствии с ИСО/МЭК 19794, где нет регламента на запись данных за исключением того, что размер в битах должен быть кратным восьми. Запись биометрической информации основана на блоке биометрических данных, но с дополнительными метаданными: дата снятия, срок хранения, данные о внешнем считывающем устройстве и др. В ИСО/МЭК 19785 устанавливаются форматы записей биометрической информации для некоторых биометрических характеристик, а также регламентируется использование записей биометрической информации для обмена биометрической информацией в рамках БиоАПИ.

Запись биометрической информации представляет собой стандартный биометрический заголовок, один или несколько блоков биометрических данных с дополнительными данными (для мультибиометрической аутентификации) и возможный блок защиты информации. Стандартный биометрический заголовок состоит из данных и абстрактных значений, определённых в стандартах, которые могут устанавливаться в соответствии с требованиями производителя (биометрической организации). В ИСО/МЭК 19785 устанавливается полный набор элементов данных и их абстрактных значений; специальные идентификаторы биометрических организаций, блоков биометрических данных и записей биометрической информации; форматы записей биометрической информации; размеры заголовков и способы их записи (бинарный или в формате XML).

В соответствии со своей разработанной архитектурой [21, 22] биометрические данные могут проходить следующие этапы обработки:

- Локальная обработка исходных образцов с целью шумоочистки, фильтрации и др.
- Сжатие образцов для уменьшения объема передаваемых данных. Общих требований или стандартов на сжатие не предъявляется. Сжатие может приводить к потери качества, и здесь нужно руководствоваться только общими рекомендациями по уменьшению ущерба качества при обработке сигнала или изображения.

• Обработка и извлечение признаков для формирования шаблона в рамках требований стандартов к блоку биометрических данных или к записи биометрической информации.

• Биометрический образец может быть передан или сжат с потерей качества, для устранения этой проблемы следует использовать кодирование биометрических данных.

• Для защиты подлинности, целостности и конфиденциальности хранимых и передаваемых биометрических данных следует использовать методы кодирования, шифрования и вставку меток времени и идентификаторов. Для этого может быть использован блок защиты информации.

Соблюдение спецификаций архитектуры БиоАПИ позволяет использовать компоненты биометрической системы разных производителей и обеспечивать их взаимодействие посредством разработанных программных интерфейсов приложений [21, 22]. Это еще одно из требований, которое было выполнено при разработке протокола обмена биометрическими данными.

4.2. Протокол обмена мультибиометрическими данными

В работе [3] предложен подход к созданию высокопроизводительных мультибиометрических технологий и систем на базе сервисно-ориентированной архитектуры, и, в частности, предложен протокол взаимодействия. Однако данный подход не учитывает большинство современных требований стандартов к разработке биометрических систем.

Спецификации БиоАПИ предназначены для определения общего интерфейса с целью предоставления возможности взаимодействия различных приложений от разных производителей и различных компонентов посредством передачи записи биометрической информации.

Стандарт протокола межсетевого обмена БиоАПИ ИСО/МЭК 24708 представляет собой требования для корректного применения линейной битовой связи, при этом программный код должен основываться на архитектуре БиоАПИ и вызове функции с определенными параметрами.

В соответствии со своей разработанной архитектурой [21, 22] в состав клиентского компонента были включены (Рис. 3): модуль обмена данными, пользовательский интерфейс, модуль формирования шаблона, внешние считывающие устройства, клиент биометрической аутентификации. В состав серверного компонента были включены (Рис. 4): модуль обмена данными, модуль управления и мониторинга, модуль принятия решения, модуль решения, модуль обращения к базе данных, сервер биометрической аутентификации.

Каждый из этих компонентов был реализован в соответствии с указанными требованиями стандартов. Все взаимодействия между модулями и компонентами свелись к следующим функциям: регистрация данных, модификация данных, идентификация данных, обработка данных и запрос данных.

5. Безопасность централизованной системы избирательной мультибиометрической аутентификации

При массовом внедрении биометрических систем возникает проблема в безопасности использования таких систем, поэтому подробно рассмотрим данный важный аспект разработки централизованной системы разграничения прав доступа на основе избирательной мультибиометрической аутентификации.

В статье [19] представлен обзор существующих атак и мер защиты. Приведем все типичные атаки, связанные с угрозами на элементы системы аутентификации (Рис. 5):

1. Атака на устройство ввода.
2. Атака на канал связи между сенсором и биометрической системой.
3. Атака на параметризацию речевого сигнала.
4. Атака на канал передачи параметризованного сигнала.
5. Атака на элемент сравнения вектора параметра и шаблона.
6. Атака на элемент результат сравнения.
7. Атака на канал связи с базой шаблонов.
8. Атака на элемент регистрации пользователя.
9. Атака на канал между элементом регистрацией и базой шаблонов.
10. Атака на элемент базы шаблонов.
11. Атака на приложение.

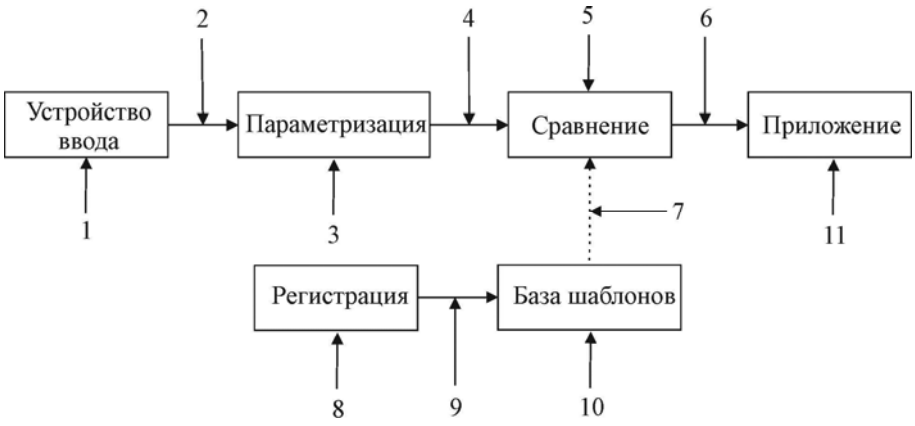

Рис 5. Общая схема биометрической аутентификации с обозначенными атаками

Все перечисленные выше атаки, кроме атаки на устройство ввода, являются общими для всех биометрических систем. Защита от подобных атак заключается в использовании цифрового кодирования, временных меток, шифрования открытого канала передачи данных, специальных методов предотвращения внедрения вредосного кода, методов антивирусной защиты и других методов защиты информации.

Больший интерес представляет атака на устройство ввода в мультибиометрической системе, так как эта атака создает реальную угрозу. Данная атака направлена на устройство ввода (сенсор) и возникает, когда злоумышленник предоставляет нелегитимные биометрические данные сенсору. Данную атаку можно разделить на три вида:

• принудительная атака — предоставление биометрических данных подлинного пользователя на нелегитимных основаниях, например, с применением насилия;

• имитационная атака — изменение биометрических характеристик злоумышленника с целью имитации биометрических данных зарегистрированного пользователя;

• атака воспроизведения — предоставление ранее записанных биометрических данных подлинного пользователя.

Многие проблемы и атаки можно предотвратить с помощью цифрового кодирования, временных меток и шифрования открытого канала передачи данных. Иными словами, создаются специальные криптографические протоколы, позволяющие предотвратить различные атаки [19].

Также для предотвращения атак можно использовать следующие методы:

• используют специальные методы обнаружения живучести биометрических образцов;

• применяют для повышения безопасности систем различные подходы к организации базы данных шаблонов и к структуре шаблона;

• используют для повышения надежности биометрических систем многофакторную аутентификацию;

• для устранения проблемы конфиденциальности и защиты информации используют специальную технологию сокращения биометрических параметров и «шифрование личности».

Анализ всех угроз на избирательную мультибиометрическую систему позволяет сделать качественный вывод, что использование мультибиометрической системы и принципа избирательности повышает надежность и безопасность системы в целом, так как атакующему необходимо учитывать все параметры и особенности реализации системы безопасности и критерии выбора всех параметров системы.

Получение количественных оценок показателей надежности и безопасности мультибиометрической аутентификации ограничивается использованием в тестировании большой базы мультибиометрических образцов, а с результатами полученных обобщенных теоретических оценок надежности можно ознакомиться в работе [12].

Заключение

В результате исследования разработана централизованная система разграничения прав доступа на основе избирательной мультибиометрической аутентификации. Предложен комбинированный подход к ее разработке, в котором используются различные критерии полуавтоматического выбора метода слияния и других параметров мультибиометрической системы аутентификации.

Важным этапом для реализации централизованной системы разграничения прав доступа на основе избирательной мультибиометрической аутентификации является разработка архитектуры системы и протокола передачи биометрических данных. В работе реализованы протоколы взаимодействия, учитывающие не только требования разработанной архитектуры системы, но и российские биометрические стандарты. Кроме того, проведен анализ возможных атак на разработанную систему, сделаны выводы и предложены рекомендации по методам защиты.

Однако существуют направления для дальнейшего развития разработанной системы: обеспечение большей универсальности, применение других биометрических характеристик, увеличение производительности и надежности, реализация динамического выбора параметров системы, в частности, метода слияния мультибиометрических данных для гарантированного уровня безопасности.

Литература

1. Сесин Е.М. Системы идентификации личности, основанные на интеграции нескольких биометрических характеристик человека / Е.М. Сесин, В.М. Белов // Доклады ТУСУРа. – № 2(25), часть 2. – 2012. – С. 175-179.
2. Ручай А.Н. Текстозависимая верификация диктора: математическая модель, статистические исследования, комплекс программ. – Saarbrucken: LAP LAMBERT Academic Publishing, 2012. – 144 с.
3. Ушмаев О.С. Сервисно-ориентированный подход к разработке мультибиометрических технологий // Информатика и ее применения. – 2008. – Т. 2. Вып. 3.– С. 41-53.
4. Ушмаев О.С. Проблемы распараллеливания биометрических вычислений в крупномасштабных идентификационных системах // Информатика и ее применения. – 2009. – Т. 3. Вып. 1. – С. 8-18.
5. Болл Р.М. Руководство по биометрии / Р. М. Болл, Дж. Х. Коннел, Ш. Панканти, Н. К. Ратха, Э. У. Сеньор. – М.: Техносфера, 2007. – 368 с.
6. Ручай А.Н. Усиление парольной аутентификации с помощью проверки ритма ввода пароля / А.Н. Ручай, А.В. Волков // Современные проблемы математики. – Екатеринбург: ИММ УрО РАН, 2013. – С. 235-237.
7. Ручай А.Н. Разработка комплекса модулей для разграничения прав доступа в ОС Windows XP на основе биометрической аутентификации // Информационные технологии и системы: материалы Первой междунар. конф. – Челябинск: ЧелГУ, 2012. – С. 75-76.
8. Ручай А.Н. Разработка универсального комплекса модулей для разграничения прав доступа в ОС Windows XP на основе биометрической аутентификации // Безопасность информационных технологии. – 2013. № 2. – С. 74-78.
9. Ручай А.Н. Формантный метод текстозависимой верификации диктора // Вестник Челяб. гос. университета. Математика. Механика. Информатика. – 2010. – № 23(204), вып. 12. – С. 121-131.
10. Ручай А.Н. Улучшение надежности формантного метода текстозависимой верификации диктора с помощью нового метода сегментации сигнала // Доклады ТУСУРа. – 2011. №2(24). – С. 241-246.
11. Ручай А.Н. Прототип централизованной системы разграничения прав доступа на основе избирательной многофакторной биометрической аутентификации // Безопасность информационных технологии. – 2013. № 1. – С. 118-120.
12. Multibiometrics for Human Identification / by editor B. Bhanu, V. Govindaraju. – Cambridge: Cambridge University Press, 2011. – 408 p.
13. Ross A.A. Handbook of multibiometrics / A.A. Ross, K. Nandakumar, A.K. Jain. – New York: Springer, 2006. – 198 p.
14. Kittler, J., M. Hatef, R. P. W. Duin, and J. Matas. On combining classifiers, IEEE Trans. Patt. Anal. Machine Intell. – 20, – 1998. – 226–239.
15. Sim, T., S. Zhang, R. Janakiraman, and S. Kumar. Continuous verification using multimodal biometrics, IEEE Trans. Patt. Anal. Machine Intell. – 29(4), 2007. – P. 687–700.
16. Frischholz, R. W., and U. Deickmann.. BioID: a multimodal biometric identification system, IEEE Comput. – 33(2). – 2000.
17. Bradlow, E. T., and P. J. Everson. Bayesian inference for the beta-binomial distribution via polynomial expansions, J. Comput. & Graphical Statistics. – 11(1). – 2002. – 200–207.
18. Poh, N., R. Wong, J. Kittler, and F. Roli. Challenges and research directions for adaptive biometric recognition systems. – Proc. ICB, Alghero, Italy. – 2009.
19. Ручай А.Н. Модель атак и защиты биометрических систем распознавания диктора // Доклады ТУСУРа. – 2011. № 1(23). – С. 96-100.
20. Dunstone T. Biometric system and data analysis: design, evaluation, and data mining / T. Dunstone, N. Yager. – Boston, Ma: Springer, 2009. – 268 p.
21. Ручай А.Н. Разработка прототипа централизованной системы избирательной многофакторной биометрической аутентификации / А.Н. Ручай, В.В. Горшенин, И.А. Маткин // Интеллектуализация обработки информации: 10-я международная конференция. Греция, о. Крит, 4-11 октября 2014 г. – М.: Торус Пресс, 2014. – С. 230.

22. Ручай А.Н. Разработка прототипа централизованной системы разграничения прав доступа на основе избирательной многофакторной биометрической аутентификации // Современные проблемы математики и ее приложений: труды 45-й Международной молод. школы-конф. – Екатеринбург: Издательство Учебно-методический центр УПИ, 2014. – С. 183-186.

Ручай Алексей Николаевич. Доцент ФГБОУ ВПО «Челябинский государственный университет». Окончил ФГБОУ ВПО «Челябинский государственный университет» в 2008 году. Кандидат физико-математических наук, старший научный сотрудник. Автор 39 печатных работ и одной монографии. Область научных интересов: биометрия, криптографические методы защиты информации, мультибиометрия, мультимодальные биометрические данные, мультисенсорная информация, обработка сигналов и изображений, распознавание образов. E-mail: ruchai@pochta.ru

Кузнецов Владислав Владимирович. Старший научный сотрудник ФГБОУ ВПО «Челябинский государственный университет». Окончил Московский государственный университет им. Ломоносова в 2010 году. Кандидат технических наук. Автор 9 печатных работ. Область научных интересов: биометрия, криптография, защищённая биометрия, нечёткие экстракторы, мультимодальные биометрические данные, обработка информации в технических системах в реальном времени, мультисенсорная информация, локализация, идентификация, фильтрация, восстановление информации.
E-mail: k.v.net@rambler.ru

Мельников Андрей Витальевич. Директор Института информационных технологий ФГБОУ ВПО «Челябинский государственный университет». Окончил Челябинский политехнический институт им. Ленинского комсомола (Южно-Уральский государственный университет) в 1978 году. Доктор технических наук. Автор 28 печатных работ и двух монографий. Область научных интересов: прикладная лингвистика, анализ тексты и системы извлечения информации из текста на русском языке, распознавание образов, обнаружение, классификация, локализация, слежение за объектами.
E-mail: mav@csu.ru

Вохминцев Александр Владиславович. Заведующий лабораторией ФГБОУ ВПО «Челябинский государственный университет». Окончил Южно-Уральский государственный университет в 2000 году. Кандидат технических наук, старший научный сотрудник. Автор 28 печатных работ. Область научных интересов: цифровая обработка информации, восстановление искаженных изображений, алгоритмы сопоставления и регистрации изображений (облаков точек), методы одновременной навигации и составления карты в неизвестном пространстве, распознавание личности по лицу на основе мультисенсорных биометрических данных. E-mail: vav@csu.ru