Инструментальный комплекс анализа движения глаз для задач интерактивной рефлекторной идентификации

En **Analysis of Eye Movement Tool Complex for Tasks of Interactive Reflex Identification**

V. A. Konyavskiy,
PhD (Eng., Grand Doctor)
konyavskiy@gmail.com

S. N. Petrov
petrovsnwm@gmail.com

S. A. Trenin
s.trenin@gmail.com

A. V. Samosyuk
alexeysamosyuk@gmail.com

Moscow Institute of Physics and Technology

I. A. Abdullaeva
a.irene.a@mail.ru

Bauman Moscow State Technical University

The most convenient way of identification is using biometric features. But the methods of biometric identification developed for forensic purposes turned out to be unsuitable for use in information systems of the digital economy, since client smartphones cannot be trusted, and therefore the static biometric characteristics that are usual for forensics cannot be used. The use of eye movement in an interactive identification system is proposed. To study the features of eye movement during stimulation with random stimuli, an instrumental complex has been created.

Keywords: biometrics, interactive reflex biometrics, digital economy, biometric identification, data set for identification, remote diagnostics

Смысл цифровой экономики – оказание услуг по принципу «здесь и сейчас» – там и тогда, когда услуга нужна, а не там, где ее удобно предоставить монополисту, коммерческому или государственному. Чтобы оказать услугу, нужно, как минимум, знать, кому она оказывается. Иными словами – идентифицировать участника цифровой экономики.

Наиболее удобный способ идентификации – это использование биометрических признаков. Но при этом мы сталкиваемся с огромной проблемой: разработанные для криминалистических целей методы биометрической идентификации оказались непригодны для использования в информационных системах цифровой экономики, так как клиентские смартфоны не являются доверенными, и поэтому статичные биометрические характеристики, привычные для криминалистики, не могут использоваться в новой экономике.

Предложено использование движения глаз в интерактивной системе идентификации. Для изучения особенностей движения глаз при стимуляции случайными стимулами создан инструментальный комплекс.

Ключевые слова: биометрия, интерактивная рефлекторная биометрия, цифровая экономика, биометрическая идентификация, дата-сет для идентификации, дистанционная диагностика

Валерий Аркадьевич Конявский,
доктор технических наук, ведущий научный сотрудник
konyavskiy@gmail.com

Сергей Николаевич Петров
petrovsnwm@gmail.com

Сергей Алексеевич Тренин
s.trenin@gmail.com

Алексей Владимирович Самосюк,
научный сотрудник
alexeysamosyuk@gmail.com

Московский физико-технический институт

Ирина Альбертовна Абдуллаева
a.irene.a@mail.ru
Московский государственный технический университет им. Н. Э. Баумана

Интерактивная рефлекторная идентификация

Источник методов биометрической идентификации – криминалистика, одной их задач которой и является идентификация субъектов, не расположенных к сотрудничеству [1]. При этом применяются хорошо разработанные методы, основанные на использовании статических характеристик и доверенных устройств. С развитием информационных систем цифровой экономики меняется сама суть подхода – клиентские устройства (смартфоны) не являются доверенными и вряд ли когда-нибудь таковыми станут. Методы удаленной (дистанционной) биометриче-

ской идентификации, основанные на статических биометрических характеристиках (папиллярном узоре, венозном рисунке, радужной оболочке и др.), принципиально уязвимы из-за возможности копирования и подмены любого из показателей, что не составит труда для злоумышленника при использовании недоверенных клиентских устройств.

Для получения услуг в цифровом виде криминалистические методы неприменимы. Изменилась основная задача: из криминалистической она стала цифровой, а в цифровом обществе субъект готов к сотрудничеству, чтобы получить необходимую ему услугу, но зато устройства – недоверенные. Необходима разработка нового подхода к идентификации, свободного от уязвимостей, присущих известным методам.

В [2–4] предложена общая схема работы системы интерактивной рефлекторной идентификации (ИРИ), устойчивой к подмене идентификатора даже при использовании недоверенных терминалов. В графическом виде эта схема отображена на рис. 1.

В проиллюстрированном сценарии пользователь хочет воспользоваться удаленным сервисом: совершить банковскую транзакцию или проголосовать. Центр обработки данных считается доверенным, в то время как доверенность пользовательского устройства гарантировать нельзя. Процедура интерактивной идентификации для наглядности условно разделена на шесть шагов. Текст черного цвета на схеме отображает названия шагов. Промежуточный обмен данными обозначен стрелками, их направление и последовательность указывают на порядок выполнения основных шагов. Здесь предполагается, что пользователь следит взглядом за стимулом на экране, и рассогласование положения стимула и взгляда характеризуют пользователя.

Использование рандомизированных стимулов исключает возможность атаки имитацией (запись реакции и ее повторное воспроизведение). В предложенной схеме задача злоумышленника (осуществить подмену идентификатора) оказывается эквивалентна по сложности задаче построения вычислительно реализуемой предсказательной модели поведения нервной системы человека. На сегодняшний день подобных моделей не существует.

Основой для реализации самого механизма идентификации должна стать новая модель идентификации человека по паре «стимул – реакция». Вопрос о том, содержится ли в данных о реакциях зрачков человека на визуальные стимулы информация, достаточная для его идентификации, обсуждался в литературе. В частности, в работе [5] показана возможность создания нейросетевой модели, позволяющей идентифицировать человека с оценкой частоты правильной идентификации 60 % на данных активного устройства слежения за направлением взгляда при частоте кадров 1000 Гц.

Подчеркнем, что невысокая, казалось бы, точность достаточна для признания того факта, что в движениях глаз содержится информация, необходимая для идентификации. Точность можно повышать, главное – информация есть. Отметим при этом, что частота кадров в использованном активном устройстве слежения очень высока, и пока недостижима для смартфонов.

Для повышения точности, снижения требований к частоте кадров при регистрации реакций и анализа устойчивости модели к атакам на биометрическое предъявление необходима разработка инструментального комплекса (ИК) для сбора данных о реакциях людей при наблюдении за случайными стимулами и анализа движений глаз (АДГ) как носителя информации для идентификации.

Основные задачи инструментального комплекса можно сформулировать следующим образом:

- *задача 1:* оценить возможность идентификации человека по активно стимулированному движению глаз и иметь возможность проводить исследования по выбору наилучшего семейства стимулов для использования в системе ИРИ;
- *задача 2:* производить регистрацию необходимой информации с помощью пассивного оборудования (RGB-камеры) параллельно с регистрацией информации с активного сенсора (инфракрасного трекера), чтобы впоследствии перейти к съему данных с использованием камеры смартфона;
- *задача 3:* осуществлять предварительную обработку данных и их визуализацию с целью устранения систематических погрешностей и формировать наборы данных для разработки улучшенных моделей идентификации.

На основе описанных задач можно предъявить набор основных требований к экспериментальному образцу комплекса. Эти требования, сгруппированные по принадлежности к различным информационным объектам и процессам, перечислены ниже.

Т1. Требования к данным

Т1.1. ИК должен поддерживать работу с различными типами стимулов, а также сохранять ассоциированную с данными АДГ информацию о стимулах. Выполнение данного требования обеспечит для исследователей возможность выбора наиболее подходящего набора стимулов, а также использование авто-

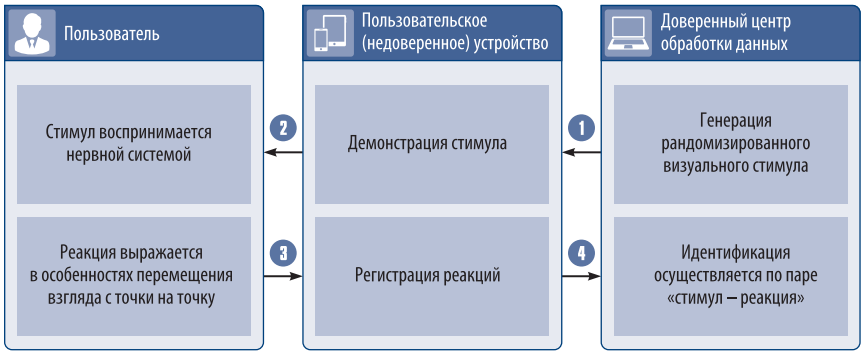

Рис. 1. ***Общая схема работы системы рефлекторной интерактивной идентификации***

матически генерируемых стимулов, необходимых для защиты от атак имитации.

Т1.2. Должна быть обеспечена возможность регистрации информации о реакциях испытуемого на стимулы с использованием пассивных и активных сенсоров.

В реальных условиях для идентификации будет использоваться камера смартфона, но эти камеры не обладают достаточной точностью. В составе ИК АДГ ИРИ активные сенсоры (трекеры) используются для получения наиболее точной информации о реакциях пользователя, а информация из пассивных (камера) – для моделирования условий реальной эксплуатации.

Т1.3. При одновременной работе активных и пассивных сенсоров в составе инструментального комплекса должна сохраняться информация, достаточная для синхронизации данных о стимуле и регистрируемых реакциях.

Для анализа необходимо использовать сенсоры разной частоты, а также стимулы динамической природы. При этом крайне важной становится задача синхронизации измерений. Корректно собранная информация о времени регистрации каждого состояния важна для дальнейшего использования данных в процессе исследования.

Т2. Требования к организации процедуры сбора данных

Т2.1. Архитектура комплекса должна предусматривать сбор данных на большом количестве разных стационарных пунктов. Выполнение требования обеспечивает осуществление параллельного сбора больших наборов данных.

Т2.2. В процессе испытаний требуется сохранять информацию, достаточную для определения ассоциированности данных с конкретным экспериментом и испытуемым, а также конфигурацию стенда. Это позволит учесть особенности конфигурации конкретного стенда и устранение возможных систематических погрешностей, а также обеспечит сбор информации о реакциях одного и того же испытуемого в разное время.

Т3. Требования к хранению и предварительной обработке данных

Т3.1. Внутренние форматы хранения должны содержать всю информацию об эксперименте и «сырые» (необработанные) данные, в том числе полные видеозаписи и демонстрируемые стимулы.

Наличие данных непосредственно с сенсоров позволит быть уверенными в том, что в процессе предобработки не будет потеряна информация, необходимая для идентификации. «Сырые» данные позволят вырабатывать механизмы предобработки, не снижающие качества идентификации.

Т3.2. Осуществление поиска, предобработки, визуализации записанных видеоданных и данных о движении глаз с целью устранения систематических погрешностей, а также их обработки при выделении информации о реакции испытуемого.

Реализация требований обеспечит подготовку набора данных с целью его опубликования. В свою очередь, доступность наборов данных для широкого круга исследователей значительно расширит возможности анализа, так как сбор данных представляет собой длительный и трудоемкий процесс, не всегда доступный при проведении дальнейших исследований.

Т3.3. Способы выделения из видеопотока информации о реакциях должны допускать использование различных алгоритмов обработки изображений. Набор алгоритмов обработки определяется задачами исследования. ИК АДГ ИРИ должен позволять применение любых доступных алгоритмов обработки изображения для выявления информации о реакциях.

Т3.4. Исследователю – пользователю комплекса – должна быть предоставлена возможность выбора набора полей для выгрузки данных при дальнейшем анализе. Выполнение этого требования позволяет деперсонализировать данные при необходимости их размещения во внешних источниках, а также сократить объем данных для дальнейшего анализа.

Архитектура комплекса

На рис. 2 отображена функциональная декомпозиция ИК. Компоненты комплекса разделены между стендом сбора данных и автомати-

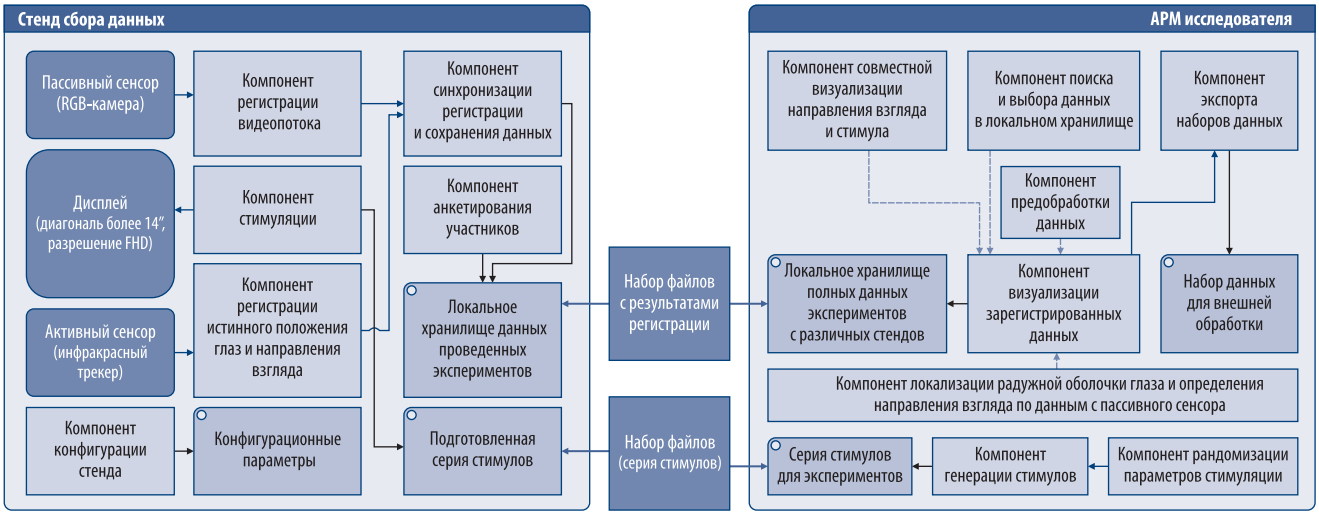

Рис. 2. ***Архитектура ИК АДГ ИРИ***

зированным рабочим местом (АРМ) исследователя. Такая декомпозиция позволяет организовать несколько пунктов сбора данных (Т2.1).

Обмен данными между стендом сбора данных и АРМ исследователя выполняется посредствам передачи файлов во внутреннем формате, который позволяет сохранить полную информацию о реакциях испытуемых и соответствующих стимулах в файловой системе стенда (Т3.1). Конвенция наименований в структуре директорий позволяет определить дату и стенд, на котором проводился сбор данных, при этом в отдельных файлах сохраняются анкетные данные испытуемого (Т2.2).

Использование в составе комплекса RGB-камеры и инфракрасного трекера позволяет осуществлять запись информации о реакциях с использованием пассивного и активного сенсоров (Т1.2).

Выделение функции локализации радужной оболочки глаза и определения направления взгляда по данным с пассивного сенсора в отдельный компонент дает возможность при необходимости организовать замену алгоритмов обработки изображений для ее реализации (Т3.3). При достижении достаточного качества реализации указанной функции архитектура позволяет полностью отказаться от использования активного сенсора, что существенно упростит и удешевит сбор данных.

Технический и программный состав ИК АДГ ИРИ

В соответствии с архитектурой, в состав ИК входит входят стенды сбора данных и рабочие места исследователей.

На рис. 3 представлено схематическое изображение стенда сбора данных. Участники эксперимента должны размещаться на расстоянии 50–90 см от экрана с диагональю не менее 14 дюймов и разрешением 1920×1080 пикселей.

Функциональные компоненты комплекса реализованы с помощью нескольких программных модулей. Ниже приведены наименования основных модулей и реализуемые ими функциональные компоненты[1].

Модуль генерации стимулов: *компоненты генерации стимулов и рандомизации параметров стимуляции.* Позволяет создавать визуальные стимулы разных типов для последующего использования в записи реакции испытуемого. Стимулы могут быть трех разных типов:

- статичный текст;
- матрица с буквами;
- точка, движущаяся по заданной траектории с заданной (переменной) скоростью.

Модуль позволяет настраивать скорость перемещения траектории, длительность стимула и разрешение демонстрируемого изображения. Также модуль позволяет создавать из отдельных стимулов серии, настраивать последовательность стимулов в ней, длительность отдельных стимулов, где это необходимо, и сохранять все результаты работы в удобном человекочитаемом формате (Т1.1). На рис. 4 представлен пользовательский интерфейс модуля.

Модуль отображения стимулов и регистрации реакций: *компоненты регистрации видеопотока, стимуляции, регистрации истинного положения глаз и направления взгляда, синхронизации регистрации и сохранения данных, анкетирования участников, конфигурации стенда.* Принимает на вход серии со стимулами, созданные генератором, воспроизводит их и записывает реакцию испытуемого, а именно, видеопоток с камеры и данные с инфракрасного трекера Tobi4C. Для синхронизации регистрации реакций с использованием сенсоров разной частоты и одновременной демонстрации стимулов разработан специальный компонент синхронизации (Т1.3). На рис. 5 представлен пользовательский интерфейс стенда сбора данных в процессе демонстрации стимула (движущаяся точка).

Модуль пакетной обработки и экспорта: *компоненты поиска и выбора данных в локальном хранилище,*

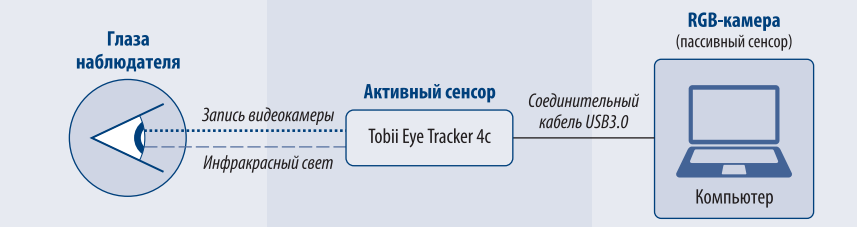

Рис. 3. ***Общая структура аппаратных компонентов стенда сбора данных***

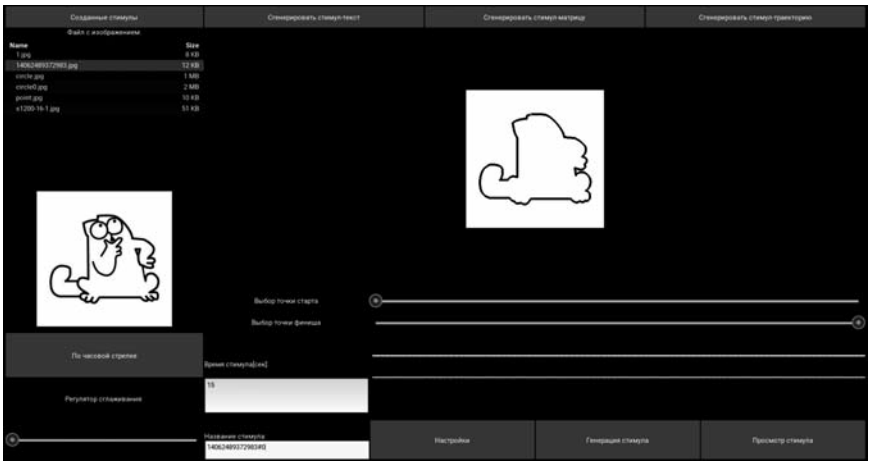

Рис. 4. ***Пользовательский интерфейс генерации стимулов (стимул – траектория)***

[1] *В разработке использовались программные продукты сторонних производителей, в том числе инструментарий Tobii Pro SDK, модули Python (poppler, pdfreader, json, numpy,random, sklearn, pandas), фреймворк визуального интерфейса kivy, библиотеки обработки изображений (opencv, dlib), приложение локализации зрачков и направления взгляда openface [6].*

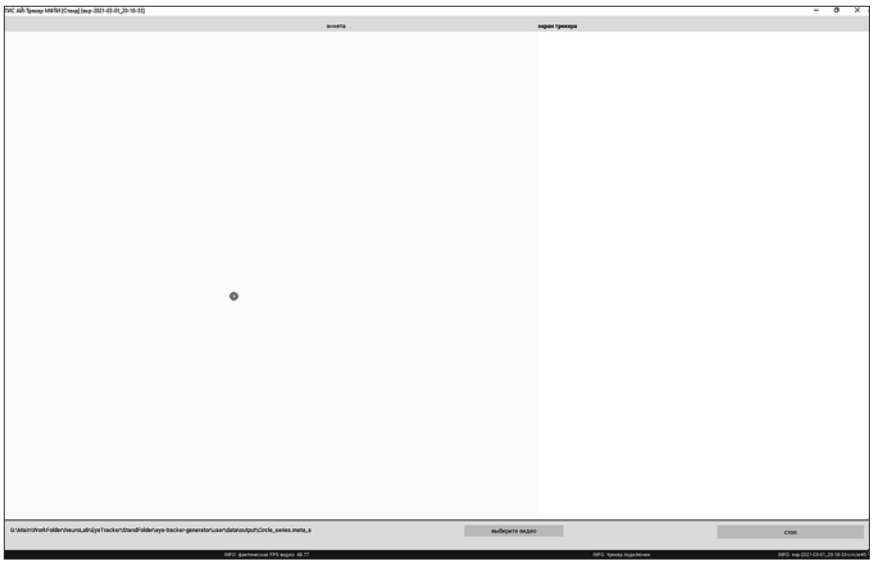

Рис. 5. ***Интерфейс стенда сбора данных (экран демонстрации стимулов)***

Рис. 6. ***Интерфейс АРМ исследователя (экран отображения траектории стимула и коррекции систематических погрешностей):***
1 – область отображения траектории;
2, 3 – список выбора траекторий слежения разных испытуемых за одинаковым стимулом,
4 – слайдеры ручной коррекции систематических погрешностей;
5–8 – элементы управления основными функциями (над ними расположен управляющий элемент перемещения по шкале времени испытания)

совместной визуализации направления взгляда и стимула, визуализации зарегистрированных данных. Предназначен для предпросмотра, сравнения и экспорта записанных данных в формат *csv*, удобный для дальнейшего анализа (Т4.1). Также он позволяет осуществлять совместный просмотр данных и расчет матриц преобразований сохраненных координат точки взгляда для устранения систематических погрешностей, вызванных возможным некорректным размещением трекера во время записи (Т3.2). На рис. 6 представлен пользовательский интерфейс модуля.

Компонент обработки видеозаписи реакции позволяет осуществлять локализацию радужной оболочки глаза на кадрах видеофайлов и определять направление взгляда испытуемого. Реализация компонента в виде отдельного программного субмодуля позволяет выполнять его простую замену для улучшения качества выполнения указанных функций.

Применение ИК АДГ ИРИ

Основная решаемая задача – создание наборов данных для дальнейших исследований. Несколько наборов данных, ориентированных на изучение особенностей рефлекторных реакций и переход к трекингу с использованием пассивных сенсоров, уже создано. В результате открыт путь к решению многих задач, в том числе:

1) интерактивной рефлекторной идентификации – на сегодня с использованием стимулов на основе замкнутых кривых Безье с геометрической непрерывностью типа G0 и G2 проведены успешные эксперименты с вероятностью успешной идентификации свыше 60 % (подробно об этом исследовании расскажем в следующей статье);

2) созданию дистанционного полиграфа;

3) дистанционной предварительной диагностики многих заболеваний определенных классов и др. ■

ЛИТЕРАТУРА

1. Конявский В. А. Новая биометрия. Можно ли в новой экономике применять старые методы? // Information Security/Информационная безопасность. – 2018. – № 4. – С. 34–36.

2. Конявский В. А. Интерактивный способ биометрической аутентификации пользователя // Патент на изобретение 2670648. 24.10.2018. Бюл. № 30.

3. Бродский А. В., Горбачев В. А., Карпов О. Э., Конявский В. А., Кузнецов Н. А., Райгородский А. М., Тренин С. А. Идентификация в компьютерных системах цифровой экономики // Информационные процессы. – 2018. – Т. 18, № 4. – С. 376–385.

4. Конявский В. А., Самосюк А. В., Тренин С. А. Рефлекторная биометрия для цифрового общества – первый шаг сделан // Information Security/Информационная безопасность. – 2020. – № 6. – С. 48–50.

5. Jäger L. A., Makowski S., Prasse P., Liehr S., Seidler M., Scheffer T. Deep Eyedentification: Biometric Identification Using Micro-movements of the Eye // Machine Learning and Knowledge Discovery in Databases, ed. Ulf Brefeld et al. Cham: Springer International Publishing, 2020. P. 299–314.

6. Baltrusaitis T., Zadeh A., Lim Y. C., Morency L. OpenFace 2.0: Facial Behavior Analysis Toolkit// 2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018), Xi'an, China, 2018. P. 59–66.