

НЕКОТОРЫЕ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ПОВЕДЕНЧЕСКОЙ БИОМЕТРИИ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

С учетом современных российских условий санитарно-эпидемиологического (ношение медицинских масок, перчаток), климатического (укутывание лиц шарфами, повязками), культурного (ношение элементов национальных костюмов, скрывающих лицо у женщин, или модных тенденций в виде щетин и бород у мужчин) характера, а также разработанных уже преступниками методов фальсификации и противодействия наиболее перспективным представляется криминалистическое исследование динамических признаков внешнего облика в виде цифрового поведения. К числу последних в первую очередь необходимо отнести стилometriю (клавиатурный почерк) – набор динамических характеристик при нажатии на клавиши клавиатуры компьютера, включающий в себя систему подсознательных автоматических действий, привычных пользователю. Кроме этого, к числу наиболее значимых признаков цифрового поведения относятся цифровой почерк, жестикация, мимика и движение губ. Выявление и исследование вышеперечисленных способов осуществляются посредством применения метода поведенческой биометрии, возможностям которого посвящена статья.

Ключевые слова: габитоскопия; внешний облик; цифровой образ; поведенческая биометрия; биометрия поведения; стилометрия; клавиатурный почерк; цифровой почерк; цифровые следы; расследование киберпреступлений; криминалистическая техника.

E.I. Foigel

SOME POSSIBILITIES OF USING BEHAVIORAL BIOMETRICS IN CRIME INVESTIGATION

Taking into account modern Russian conditions of sanitary and epidemiological (wearing medical masks, gloves), climatic (wrapping faces with scarves, bandages), cultural (wearing elements of national costumes that hide the face in women or fashion trends in the form of bristles and beards in men) character, and also developed by criminals methods of falsification and counteraction, the most promising is the forensic study of dynamic signs of external appearance in the form of digital behavior. Among the latter, first of all, it is necessary to include stylometry (keyboard handwriting) – a set of dynamic characteristics when pressing the keys of a computer keyboard, which includes a system of subconscious automatic actions familiar to the user. In addition, digital handwriting, body language, facial expressions, and lip movement are among the most significant signs of digital behavior. The identification and study of the above methods is carried out with the help of the method of behavioral biometrics, the capabilities of which the article is devoted to.

Keywords: habitoscopy; physical appearance; digital imaging; behavioral biometrics; behavior biometrics; stylometry; keyboard handwriting; digital handwriting; digital footprints; cybercrime investigation; forensic techniques.

Глобальная цифровизация, проникающая во все сферы общественной жизни, неожиданно стала основным средством решения серьезных проблем, с которыми столкнулось человеческое общество в реалиях пандемии новой коронавирусной инфекции. Своевременно принятая Стратегия развития информационного общества в Российской Федерации на 2017–2023 годы, утвержденная указом Президента Российской Федерации от 9 мая 2017 г. № 203, закрепила необходимость обеспечения всеобщего доступа к информационным и коммуникационным технологиям и интенсификации использования самих технологий, обеспечив их широкое внедрение в большинство сфер общественной жизни. Применение активно появляющихся в последнее время научных разработок требует соответствующего научного обоснования. Не стала исключением и криминалистическая наука.

Представляется, что к числу наиболее перспективных научных разработок можно отнести поведенческую биометрию – метод, с помощью которого происходит распознавание цифрового почерка и цифрового поведения.

Стилометрия (клавиатурный почерк) – это набор динамических характеристик при нажатии на клавиши клавиатуры компьютера, включающий в себя систему подсознательных автоматических действий, привычных пользователю. Наиболее важными из них являются: динамика ввода (время между нажатием клавиш и временем их удержания), скорость набора (время, которое требуется пользователю для поиска нужного символа на клавиатуре), скорость ввода (результат деления количества символов на время печатания), интенсивность нажима (сила воздействия на клавишу клавиатуры), продолжительность и структура пауз и задержек, особенности реализации клавиш (использования клавиш для печатания определенных знаков – заглавных букв, кавычек, скобок и т.д.), частота ошибок при вводе.

Несмотря на относительную молодость данного способа, по оценкам исследователей, вероятность идентификации пользователя по клавиатурному почерку – 0,91 [1]. Исследование клавиатурного почерка имеет ряд преимуществ: невозможность передачи другому человеку (в отличие от секретного кода, шифра, ключа), отсутствие необходимости в применении сложной дорогостоящей аппаратуры, незаметность проверки для пользователя. Клавиатурный почерк предоставляет широкие возможности при диагностике цифрового автоподлога – ситуации, при которой недобросовестный пользователь инсценирует хищение личностной информации третьими лицами (например, лично осуществив списание со своего счета, утверждает, что стал жертвой мошенничества вследствие неправомерного доступа к банковскому счету).

Основной принцип распознавания клавиатурного почерка сводится к тому, что пользователю предлагается набрать контрольную фразу (текст), исследуемую с помощью различных методов, в основе которых лежит исследование времени между событиями клавиатуры (т.е. нажатием кнопки и ее отпусканием). Идентификация пользователя строится на анализе длительности интервалов, соответствующих каждой комбинации клавиш [2, с. 179].

Клавиатурный почерк является наиболее значимой разновидностью *цифрового почерка*, в который, помимо закономерностей использования клавиш

компьютерной клавиатуры, входят еще такие характеристики, как закономерности движения компьютерной мышью (особенности использования клавиш и колесика, их сочетание, амплитуда и радиус движения компьютерной мыши), навигационные привычки, а также особенности использования тачскрина смартфона (скорость, стиль взаимодействия и давления и т.д.).

Жестикуляция, мимика, движения губ. В отличие от традиционных одноименных динамических признаков внешнего облика, жесты, мимика и движения губ как часть цифрового поведения человека фиксируются с помощью веб-камер или камер наружного наблюдения и представляют собой сформированные привычные движения при манипуляциях с компьютерной техникой и цифровыми устройствами. Так, форма движения губ при произнесении кодового слова, цифрового пароля с учетом структуры и мимики обладает индивидуальностью и выражается в особенностях видимой артикуляции, при этом внимание обращается не на смысловое содержание слова, пароля и его соответствие заданному, а именно на внешнее выражение речевой активности.

Жестикуляция как элемент цифрового поведения человека выражается в движениях рук при манипуляциях с цифровым устройством мобильного характера (чаще всего смартфона). Имеет значение угол, под которым удерживается смартфон, значение пальцев, которые использует подозреваемый для управления приложениями в гаджете, жесты и движения по управлению телефоном, а также паузы между ними.

Все упомянутые элементы цифрового поведения человека фиксируются и распознаются с помощью биометрического метода и получили название «биометрия поведения» («поведенческая биометрия» [3], «пассивная биометрия», «тихая биометрия») [4]. Как и при традиционном методе криминалистической идентификации, в основе биометрии поведения лежит сравнение выявленной совокупности индивидуальных устойчивых признаков, характеризующих поведение лица (их подсчет, измерение и статистический анализ), с контрольными образцами, которые, как правило, хранятся в информационной базе данных. Применение математических и статистических методов при этом осуществляется специалистом посредством использования электронно-вычислительной техники.

К плюсам поведенческой биометрии можно отнести скрытый характер – испытуемый может не подозревать, что осуществляется фиксация его поведенческих характеристик, поскольку ему не объявляют о необходимости предъявить какие-либо факты либо осуществить какие-либо действия – он просто ведет себя естественно. Скрытый характер удобен для создания базы данных – не нужно осуществлять какие-либо технически сложные действия, привлекать большое количество специалистов.

Естественность поведения испытуемого – обстоятельство, которое обуславливает невозможность фальсификации поведенческих характеристик. Если отпечатки пальцев, форму лица и иных частей тела можно искусственно сконструировать, используя машинные методы, то поведение человека скопировать и воссоздать невозможно, поскольку оно комплексно, динамично и индивидуально.

Научная обоснованность метода поведенческой биометрии должна основываться на соответствии деятельности ГОСТам, регламентирующим испытания биометрических технологий: ГОСТ Р ИСО/МЭК 19795-1-2007 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура» (утвержден приказом Федерального агентства по техническому регулированию и метрологии от 25 декабря 2008 г. № 403-ст) и ГОСТ Р ИСО/МЭК 19795-2-2008 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 2. Методы проведения технологического и сценарного испытаний», (утвержден приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 448-ст).

Использование метода поведенческой биометрии позволит решить идентификационные задачи и достичь поисковые цели, а также решить некоторые диагностические задачи – получить информацию о состоянии лица, его положении, возрасте, поле и других характеристиках.

Список использованной литературы

1. Григорьев В.Р. Использование статических методов для биометрической идентификации пользователя / В.Р. Григорьев, А.П. Никитин // Вестник РГГУ. Сер.: Информатика. Защита информации. Математика. – 2012. – № 14. – С. 135–142.

2. Иванов Д.А. Противодействие анализу клавиатурного почерка / Д.А. Иванов, А.П. Никитин // Вестник РГГУ. Сер.: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. – 2014. – № 11 (133). – С. 178–183.

3. Behavioural biometrics: Online identification is getting more and more intrusive // The Economist. – 2019. – May. – URL: <https://www.economist.com/science-and-technology/2019/05/23/online-identification-is-getting-more-and-more-intrusive>.

4. Liang Wang, Xin Geng. Behavioural biometrics for human identification: intelligent Application / Wang Liang, Geng Xin. – Hershey : Medical Information Science Reference, 2010. – 505 p.

Информация об авторе

Фойгель Елена Игоревна – кандидат юридических наук, доцент, кафедра криминалистики, судебных экспертиз и юридической психологии, Институт государства и права, Байкальский государственный университет, г. Иркутск, Российская Федерация, e-mail: FojgelEI@bgu.ru.

Author

Foigel, Elena I. – Ph.D. in Law, Ass. Professor, Department of Criminalistics, Forensics and Legal Psychology, Institute of State and Law, Baikal State University, Irkutsk, the Russian Federation, e-mail: FojgelEI@bgu.ru.