Обзорная статья
УДК 004.056
DOI:10.31854/1813-324X-2023-9-5-91-111

Обзор методов идентификации пользователя на основе цифровых отпечатков

Андрей Владимирович Осин, a.v.osin@mtuci.ru
Юрий Викторович Мурашко ✉, u.v.murashko@edu.mtuci.ru

Московский технический университет связи и информатики,
Москва, 111024, Российская Федерация

Аннотация: *Рассмотрены методы идентификации пользователей на основе цифровых отпечатков. Представлены основные подходы для формирования последних для браузера, который установлен на пользовательском устройстве и характеризует его принадлежность. Также описаны методы, применяемые для идентификации человека (пользователя) в процессе эксплуатации устройства. Представлены методы, использующие как динамику нажатий клавиш и взаимодействий с сенсорным экраном, голосовые и геолокационные данные, так и поведенческую биометрию и поведенческий профиль. В качестве развития подхода идентификации описана концепция непрерывной аутентификации. Приводится список общедоступных наборов данных, упоминаемых в рассмотренных в обзоре исследованиях, с указание ссылок для их скачивания. Приводится обширный список работ, отражающих современное состояние исследований в области цифровых отпечатков.*

Ключевые слова: *идентификация, цифровой отпечаток, браузер, поведенческая биометрия, непрерывная аутентификация*

Ссылка для цитирования: Осин А.В., Мурашко Ю.В. Обзор методов идентификации пользователя на основе цифровых отпечатков // Труды учебных заведений связи. 2023. Т. 9. № 5. С. 91–111. DOI:10.31854/1813-324X-2023-9-5-91-111

A Review of User Identification Methods Based on Digital Fingerprint

Andrey Osin, a.v.osin@mtuci.ru
Yuri Murashko ✉, u.v.murashko@edu.mtuci.ru

Moscow Technical University of Communications and Informatics,
Moscow, 111024, Russian Federation

Abstract: *Methods of user identification based on digital fingerprints are considered. The main approaches for the browser fingerprints creation which is installed on the user's device and characterizes the device belonging to the user are presented. The methods used to identify a person (user) during the operation of the device are also described. Methods using both the dynamics of keystrokes and interactions with the touch screen, voice and geolocation data, as well as behavioral biometrics and behavioral profile are presented. The concept of continuous authentication is described as a development of the identification approach. A list of publicly available data sets mentioned in the studies reviewed in the review is provided, with links to download them.*

Keywords: *identification, digital fingerprint, browser, behavioral biometrics, continuous authentication*

For citation: Osin A., Murashko Y. A Review of User Identification Methods Based on Digital Fingerprint. *Proceedings of Telecommun. Univ.* 2023;9(5):91–111. DOI:10.31854/1813-324X-2023-9-5-91-111

Введение

Развитие средств вычислительной техники и связи позволило собирать, хранить, обрабатывать и передавать информацию в таких объемах и с такой оперативностью, которые были немыслимы раньше. Современный этап информатизации связан с повсеместным использованием персональной электронно-вычислительной техники, систем телекоммуникаций, сетей ЭВМ. Поэтому возрастает потребность в разработке и применении эффективных решений в сфере информационной безопасности. Под информационной безопасностью в общем виде следует понимать совокупность средств, методов и процессов (процедур), обеспечивающих защиту информационных активов и, следовательно, гарантирующих сохранение эффективности и практической полезности как технической инфраструктуры информационных систем, так и сведений, которые в таких системах хранятся и обрабатываются.

В данной статье рассматривается один из таких процессов обеспечения информационной безопасности – идентификация. Это процедура распознавания субъекта по его уникальному идентификатору, присвоенному ему ранее и занесенному в базу данных в момент его регистрации в качестве легального пользователя системы. В качестве распознаваемого субъекта может выступать физическое лицо, учетная запись компьютерной сети предприятия или, например, активность в трафике. Идентификатором субъекта могут выступать различные технологии, например, физические ключи доступа, биометрия, имя пользователя, файлы cookie, атрибуты трафика (IP-адрес, порт и др.).

Однако существуют методы фальсификации подобных идентификаторов, поэтому появляется необходимость в сборе данных для идентификации, где изменение одного или нескольких параметров не окажет большого воздействия на процесс идентификации. Для решения этой задачи может быть использована концепция цифрового отпечатка. Цифровой отпечаток – это информация, собранная, например, об удаленном устройстве для его идентификации. Поскольку данная концепция универсальная, то алгоритм на ее основе может быть применен во многих областях, например, для предотвращения мошенничества [1], формирования целевой рекламы [2], классификации вредоносного трафика [3], предотвращения обхода блокировок с использованием средств анонимизации [4], защита авторских прав [5–7] и др.

1. Идентификация на основе цифрового отпечатка браузера

Одна из самых распространенных областей, где используется цифровой отпечаток – идентификация браузера пользователя на основе собранных данных различными технологиями отслеживания при посещении какого-либо сайта. Необходимость использования именно цифрового отпечатка обусловлена тем, что такие идентификаторы, как файлы cookie, возможно обойти, а фальсифицировать весь массив данных, собранных о браузере, намного сложнее.

1.1. Исследования цифрового отпечатка браузера

В 2010 г. П. Экерсли из Electronic Frontier Foundation провел эксперимент с использованием программы Panopticlick [8]. Общаясь в социальных сетях и на популярных веб-сайтах, он за две недели собрал 470 161 цифровых отпечатков с данными из заголовков HTTP, JavaScript и плагинов, таких как Flash или Java. Из них 94,2 % были уникальными. Это сильно повлияло на конфиденциальность пользователей, так как браузер с редкими параметрами может быть легко идентифицирован в Интернете.

В 2012 г. в исследовании [9] была изучена возможность применения библиотеки для создания двухмерных изображений Canvas API при формировании цифрового отпечатка браузера. В исследовании отмечается, что обработка шрифтов может различаться в зависимости от устройства, поскольку операционная система, версия браузера, видеокарта, установленные шрифты, субпиксельные подсказки и сглаживание играют роль в создании окончательного видимого пользователем растрового изображения (рисунок 1). В ходе эксперимента они наблюдали 50 различных изображений из 300 образцов.

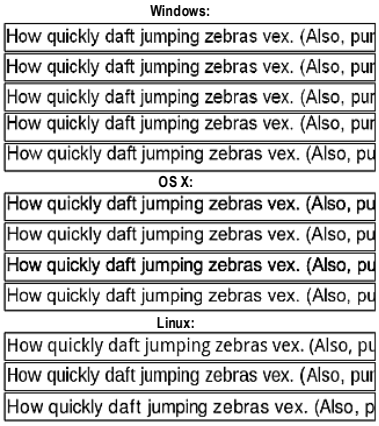

Рис. 1. Отрисовка текста с помощью Canvas API в разных операционных системах

Fig. 1. Drawing Text with Canvas API in Different Operating Systems

Также в [9] изучали использование WebGL API для получения дополнительных характеристик цифрового отпечатка браузера. Это библиотека для отображения интерактивных 3D-объектов в браузере и манипулирования ими с помощью JavaScript без необходимости использования плагинов.

В ходе эксперимента наблюдалось 50 различных отрисовок из 270 образцов, что объясняется разницей в аппаратном и программном обеспечении, при которой обработка не идентична на различных устройствах.

В 2017 г. в [10] разработан метод получения цифровых отпечатков, который также использует библиотеку WebGL при идентификации устройств. С помощью серии из 31 задачи отрисовки 3D-объектов тестируются параметры компьютерной графики для извлечения характеристик устройства, что позволило однозначно идентифицировать более 99 % из 1903 протестированных устройств.

В [11] описан еще один способ извлечения характеристик устройства для дополнения цифрового отпечатка браузер (рисунок 2). Способ основан на использовании Web Audio API, предоставляющий интерфейс для генерирования аудиосигнала и применения к нему специфических операций, таких как сжатие или фильтрация. Отмечается, что процесс получения цифровых отпечатков с использованием Web Audio API аналогичен процессу получения цифровых отпечатков с помощью Canvas API, поскольку обработанные сигналы будут иметь различия из-за программного и аппаратного обеспечения устройств.

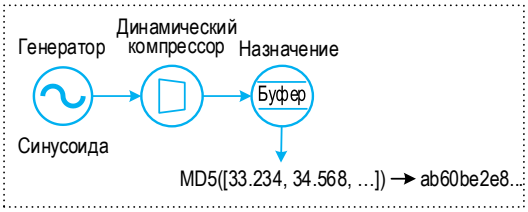

Рис. 2. Процесс извлечения характеристик с помощью Web Audio API

Fig. 2. Feature Extraction Process Using the Web Audio API

Современные браузеры предусматривают возможность разрабатывать собственные расширения, позволяющие увеличить его функциональные возможности. Однако из-за того, как расширения интегрируются в браузеры, некоторые из них можно обнаружить. Так, в исследовании [12] рассматривается механизм обнаружения расширений на основе доступности его ресурсов, например, логотипа. Поскольку доступ к таким ресурсам возможен в контексте любой веб-страницы, то можно использовать этот механизм для обнаружения наличия или отсутствия определенного расширения. Таким образом было обнаружено 12154 расширения браузера Chrome из 43429 и 1003 расширения браузера Firefox из 14896.

Похожее исследование было проведено в [13]. Авторы запрашивали ресурсы поддельных и существующих расширений и измеряли разницу во времени между вызовами (рисунок 3). Утверждается, что с помощью этого метода можно обнаружить любое расширение браузера. Авторы также провели исследование 204 пользователей с целью обнаружения 2000 расширений: они пришли к выводу, что 56,86 % пользователей уникальны.

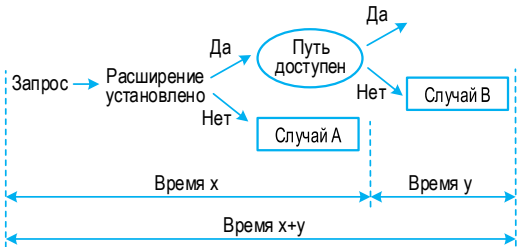

Рис. 3. Схема контроля доступности ресурсов

Fig. 3. Resource Availability Control Scheme

В [14] проведено исследование, которое заключается в выявлении побочных эффектов, вызываемых расширениями браузеров. Например, если расширение добавляет кнопку, то ее можно обнаружить путем анализа DOM (*аббр. от англ.* Document Object Model – объектная модель документа) вебстраницы (рисунок 4). В исследовании, основанном на 854 пользователях и обнаружении 1656 расширений, авторы пришли к выводу, что 14,10 % пользователей уникальны.

```
<div class="ProfileTweet-action action-pocket-container">
    <a class="js-tooltip"  href="#" data-original-title="
        Save to Pocket">
    <span class="icon icon-pocket"></span>
        </a></div>
<div class="ProfileTweet-action…
```

Рис. 4. Изменения DOM, внесенные расширением

Fig. 4. DOM Changes Made by the Extension

Еще один способ получить информацию об устройстве – сравнить возможности его центрального и графического процессоров. С помощью JavaScript можно запускать ряд задач и измерять время, необходимое для их выполнения. Однако самая большая трудность при использовании таких тестов производительности заключается в том, чтобы правильно оценить разницу и погрешность измерений. Два значения времени могут быть разными, потому что они были собраны с двух разных устройств, но они также могут принадлежать одному устройству, где появился новый фоновый процесс, нарушивший условия измерений.

В [15] использовалось 39 различных тестов для определения производительности «движка» Java Script; была показана возможность определения браузера и его версии с точностью 79,8 %. Но самым большим недостатком предложенного подхода является то, что для запуска полного набора тестов требуется в общей сложности 190,8 с. В отличие от большинства атрибутов, описанных выше, которые можно собрать за миллисекунды, эта разница во времени делает практически невозможным применение таких методов в реальных условиях.

В [16] используется библиотека WebGL API для отображения сложных 3D-сцен и измерения количества кадров, отображаемых браузером. Авторы показали, что оценка производительности графического процессора позволяет обнаружить различия между устройствами, поскольку небольшой графический процессор, например в смартфоне, будет значительно уступать в скорости выполнения операций новейшей графической карте высокого класса.

В [17] выполнен анализ конфиденциальности Battery Status API, где предоставляется такая информация об аккумуляторе устройства, как уровень его заряда, оставшееся время заряда и разряда, а также заряжается ли устройство в данный момент. Целью создания данной библиотеки было предоставление веб-разработчикам возможности реализации энергоэффективных приложений, однако в исследовании отмечается, что уровень заряда аккумулятора можно использовать в качестве краткосрочного идентификатора на сайтах, а повторные считывания могут помочь определить его емкость.

Важным аспектом цифрового отпечатка браузера является его эволюция с течением времени. Поскольку цифровой отпечаток является прямым отражением устройства пользователя и его окружения, он подвержен изменениям по мере модификации, настройки или обновления компонентов системы. Чтобы обеспечить долгосрочное отслеживание, необходимо понимать эти изменения и предвидеть, как может измениться цифровой отпечаток.

В [18] проведено обширное исследование, в ходе которого авторы ежедневно собирали цифровые отпечатки у добровольцев с помощью расширений браузеров Firefox и Chrome. По результатам исследования были выделены три типа эволюции цифровых отпечатков: автоматическая эволюция, вызванная обновлениями программного обеспечения; контекстно-зависимая эволюция, отражаемая изменениями в окружении пользователя; и эволюция, инициированная пользователем, вызванная изменением настроек браузера. Отмечается, что эволюция цифровых отпечатков браузера сильно зависит от типа устройства и того, как оно используется. Также авторы попытались со временем объединить цифровые отпечатки, принадлежащие одному и тому же устройству. Собирая цифровые отпечатки каждые три дня, их алгоритм мог отслеживать устройство в среднем 51,8 дня. Также удалось отследить 26 % устройств в течение более 100 дней, доказав, что снятие цифровых отпечатков браузера может эффективно использоваться в дополнение к другим методам идентификации.

Наиболее значимые работы в области цифровых отпечатков браузера приводятся в таблице 1.

ТАБЛИЦА 1. Основные исследования цифровых отпечатков браузера

TABLE 1. Basic Research on Digital Browser Fingerprints

Ссылка	Год	Цитируемость	Описание	Параметры
[8]	2010	1215	Electronic Frontier Foundation запустил веб-сайт, на котором посетители могут проверить цифровой отпечаток своего браузера. Собрав образцы из 470161 цифровых отпечатков, они измерили как минимум 18,1 бит энтропии, возможной при снятии отпечатков браузера.	• User Agent • HTTP ACCEPT headers • Cookie enabled? • Timezone • System fonts • Partial supercookie test
[9]	2012	406	Исследователи из Калифорнийского университета в Сан-Диего показали, как Canvas API и WebGL API можно использовать при создании цифровых отпечатков браузера.	• Canvas API • WebGL API
[11]	2016	666	Web Audio API является одним из последних дополнений в наборе инструментов получения цифровых отпечатков браузера. Обнаружены скрипты, которые обрабатывают звуковой сигнал для получения цифровых отпечатков браузера.	Web Audio API
[12]	2017	55	Исследования направлены на обнаружение расширений браузера по URL-адресам, изменению DOM веб-страницы и по разнице по времени между вызовами расширений.	Расширения браузера
[13]		89		
[14]		42		

1.2. Наборы данных

Обычно выделяют три крупномасштабных исследования по сбору цифровых отпечатков браузера, которые оказали большое влияние и способствовали развитию исследований в этой области: упомянутый ранее Panopticlick [8], AmIUnique [19] и Hiding in the Crowd [20]. В таблице 2 представлен краткий обзор этих трех масштабных исследований цифрового отпечатка браузера.

Эксперимент Panopticlick проводился в течение двух недель, в ходе которых было собрано около 470161 цифровых отпечатков браузера. Из них 83,6 % были уникальны, а если пользователи включали Flash или Java, то этот процент увеличивался

до 94,2 %. Список плагинов, список шрифтов и параметр user-agent были в то время наиболее информативными атрибутами. Также отмечается, что этот набор данных необъективен, поскольку данные получены от пользователей, которые заботятся о своей конфиденциальности в Интернете. Эти пользователи выполняли несколько простых мер, таких как ограничение файлов cookie или, возможно, использовали прокси-сервера для конфиденциального просмотра веб-страниц.

В эксперименте AmIUnique проведен анализ 118934 цифровых отпечатков браузера и выявлены новые результаты. Во-первых, подтверждены выводы исследования Panopticlick, поскольку 89,4 % собранных цифровых отпечатков браузера были уникальными. Однако за 6 лет, которые разделяют оба исследования, произошла эволюция различных атрибутов, составляющих цифровой отпечаток браузера. Если в начале десятилетия список плагинов и шрифтов были самыми информативными, то со временем сторонние плагины были отключены в основных браузерах из-за угрозы безопасности. В исследовании AmIUnique использовались полученные с помощью Canvas API параметры, энтропия которых была довольно высокой. В рамках эксперимента также были проанализированы различия между цифровыми отпечатками браузера на компьютерах и мобильных устройствах. Идентификация браузера на этих устройствах в значительной степени зависела от HTTP-заголовков и параметров, полученных с помощью Canvas API. В ходе анализа было установлено, что 81 % цифровых отпечатков браузера с мобильных устройств уникальны. Также, в исследовании обозначается, что такие простые изменения, как наличие стандартных HTTP-заголовков или удаление плагинов, снижают уникальность цифровых отпечатков браузера на компьютерах на 36 %.

В исследовании Hiding in the Crowd проанализировано 2067942 цифровых отпечатков браузера. Их результаты дают новый уровень понимания этой области, поскольку всего 33,6 % цифровых отпечатков браузера из их набора данных были уникальными. По сравнению с вышеупомянутыми исследованиями, это число в два-три раза меньше. Если рассматривать мобильные устройства, то разница еще больше: 18,5 % цифровых отпечатков браузера мобильных устройств были уникальными по сравнению с 81 % из исследования AmIUnique. Данное исследование подчеркивает важность процесса сбора данных. В прошлом цифровые отпечатки браузера собирались на веб-сайтах, ориентированных на посетителей, которые знают о конфиденциальности в Интернете или могут быть более осторожными, чем обычные пользователи. В данном случае данные собирались на коммерческом сайте, ориентированном на более глобальную аудиторию. Эта особенность набора данных в сочетании с очень большим количеством собранных цифровых отпечатков браузера являются ключом к пониманию различий в их уникальности. Также отмечается, что цифровые отпечатки браузера на компьютерах в основном уникальны из-за комбинации атрибутов, в то время как на мобильных устройствах присутствует атрибуты, имеющие уникальные значения. В таблице 3 приведена сводка атрибутов браузера вместе с их энтропией.

ТАБЛИЦА 2. Обзор исследований цифрового отпечатка браузера

TABLE 2. Overview of Browser Digital Fingerprint Studies

	Panopticlick (2010) [8]	AmIUnique (2016) [19]		Hiding in the Crowd (2018) [20]	
	Компьютер	Компьютер	Мобильный	Компьютер	Мобильный
Количество	470,161	105,829	13,105	1,816,776	251,166
Уникальность	94,2 %	89,4 %	81 %	35,7 %	18,5 %

ТАБЛИЦА 3. Атрибуты браузера и их энтропия в исследованиях цифровых отпечатков браузера

TABLE 3. Browser Attributes and Their Entropy in Studies of Digital Browser Fingerprint

Атрибуты	Panopticlick (2010)	AmIUnique (2016)	Hiding in the Crowd (2018)
	Энтропия		
Заголовок HTTP User-Agent	10,000	9,779	7,150
Заголовок HTTP Accept	–	1,383	0,729
Кодирование содержимого	–	1,534	0,382
Язык содержимого	–	5,918	2,716
Список расширений	15,400	11,060	9,485
Включены файлы cookie	0,353	0,253	0,000
Использование локального/сеансового хранилище	–	0,405	0,043

Атрибуты	Panopticlick (2010)	AmIUnique (2016)	Hiding in the Crowd (2018)
	Энтропия		
Часовой пояс	3,040	3,338	0,164
Разрешение экрана и глубина цвета	4,830	4,889	4,847
Список шрифтов	13,900	8,379	6,904
Список заголовков HTTP	–	4,198	1,783
Платформа	–	2,310	1,200
Включена функция «Не отслеживать»	–	0,944	1,919
Canvas API	–	8,278	8,546
WebGL Vendor	–	2,141	2,282
WebGL Renderer	–	3,406	5,541
Использование блокировщика рекламы	–	0,995	0,045

1.3. Применение цифровых отпечатков браузера

Цифровые отпечатки браузера могут применяться для различных целей, включая идентификацию пользователей и защиту от мошенничества. Однако следует отметить, что это может вызвать определенные проблемы, такие как нарушение конфиденциальности и приватности.

1.3.1. Отслеживание

Поскольку цифровые отпечатки браузера могут с высокой точностью идентифицировать устройства в Интернете, то последствия для конфиденциальности очень важны. Собирая цифровые отпечатки браузера на нескольких веб-сайтах, третья сторона может узнать пользователя и соотнести его активность в браузере внутри и между сессиями. При этом пользователь не может контролировать процесс отслеживания, поскольку он выполняются в фоновом режиме.

Если устройство имеет уникальный цифровой отпечаток, оно может быть идентифицировано в Интернете без использования других идентификаторов, таких как cookie файлы или IP-адрес. Пользователи, передающие свои сетевые пакеты через VPN (виртуальную частную сеть), особенно уязвимы для цифровых отпечатков браузера, поскольку VPN маскирует только IP-адрес.

В отсутствие cookie файлов цифровые отпечатки браузера можно использовать для отслеживания различных устройств, скрывающихся за одним и тем же IP-адресом.

1.3.2. Выявление уязвимостей устройства

Анализируя содержимое цифрового отпечатка браузера, злоумышленник может выявить потенциальные уязвимости, сопоставив список установленных на устройстве компонентов с базой данных распространенных уязвимостей. Затем он может разработать эффективный вредоносный код для конкретного устройства, заранее зная его уязвимости. Например, через свойство navigator.plugins можно узнать, работает ли на устройстве устаревшая версия плагина Flash, и если он не обновлен, то злоумышленник может удаленно выполнить вредоносный код на устройстве.

Компании Malwarebytes и GeoEdge в своей работе «Operation fingerprint» подробно описали, как рекламные кампании используют цифровые отпечатки браузеров для доставки вредоносных программ на уязвимые устройства [21]. Программный код цифровых отпечатков встраивается непосредственно в JavaScript поддельных рекламных объявлений и определяет, является ли устройство уязвимым или нет. Если да, то на устройстве будет показано объявление с вредоносным кодом, которое перенаправляет на набор инструментов для эксплуатации уязвимостей.

1.3.3. Повышение безопасности в Интернете

Выявление уязвимостей устройства с помощью цифровых отпечатков браузера можно применять и с целью их устранения. С помощью простого сканирования безопасности системные администраторы могут легко выявить устройства с устаревшими компонентами и быстро установить обновления.

Еще одно применение цифровых отпечатков браузера – повышение безопасности в Интернете путем проверки фактического содержания цифрового отпечатка. Поскольку между собранными атрибутами существует множество зависимостей, можно проверить, был ли отпечаток подделан или соответствует ли он устройству, которому предположительно принадлежит.

Одной из первых компаний, внедривших метод сбора цифровых отпечатков для предотвращения мошенничества в Интернете, была ThreatMetrix – компания по безопасности, специализирующаяся на проверке транзакций в Интернете [22]. Было отмечено, что мошенники меняют свой IP-адрес, удаляют cookie файлы, а программный код ботнетов произвольно изменяет атрибуты устройств. Другие компании по безопасности, такие как Imperva [23], MaxMind [24], HUMAN [25], IPQualityScore [26],

Radware [27] или Sift [28], также используют цифровые отпечатки браузера для обнаружения ботов и необычной активности.

Цифровой отпечаток браузера можно применять в дополнении к паролю для аутентификации в Интернете. Проверяя цифровой отпечаток браузера при входе в систему, можно блокировать несанкционированный доступ с новых и неизвестных устройств. Некоторые компании включают в свои продукты решения по снятию цифровых отпечатков браузера для усиления аутентификации. SecurAuth является поставщиком адаптивного решения для контроля доступа. Как часть их многофакторной аутентификации, они включают систему аутентификации на основе цифровых отпечатков устройств [29]. Другая компания под названием TransUnion имеет решение под названием TruValidate [30], которое объединяет сбор информации об устройстве в рамках многофакторной аутентификации.

2. Идентификация на основе цифрового отпечатка пользователя

Цифровой отпечаток браузера формируется из описанных ранее статических атрибутов, т. е. извлекаются однократно при подключении пользователя к веб-сайту [31]. Однако в условиях роста числа киберпреступлений идентификация на основе статических характеристик не обеспечивает достаточный уровень безопасности системе. Перехват сеанса и атака типа «человек посередине» – это всего лишь два примера потенциальных угроз, которыми может воспользоваться злоумышленник, чтобы выдать себя за легального пользователя системы, которая применяет статическую идентификацию [32]. Поэтому эксперты по безопасности в настоящее время рассматривают возможность внедрения динамической непрерывной идентификации. Непрерывная идентификация может быть выполнена с помощью поведенческой биометрии, которая является одним из наиболее перспективных решений этой проблемы. Поведенческие системы динамической идентификации в настоящее время внедряются в банках, государственных организациях и других учреждениях для обеспечения эффективной системы защиты от киберпреступлений [33].

Главное преимущество использования поведенческих характеристик заключается в возможности идентификации конкретного пользователя, а не его устройство, как, например, при использовании цифрового отпечатка браузера [34]. В зависимости от условий и поставленных задач поведенческие характеристики могут применятся по отдельности, однако объединение их в цифровой отпечаток пользователя позволит увеличить эффективность идентификации.

2.1. Исследования цифрового отпечатка пользователя

2.1.1. Динамика нажатия

Наиболее часто используемой поведенческой характеристикой является динамика нажатия клавиш клавиатуры, которую можно собрать, например, при вводе пользователем пароля. Многие существующие решения основаны на статистических данных о конкретных событиях, количестве их повторений во времени или определенных сочетаниях этих событий. Наиболее часто используемые характеристики включают: продолжительность нажатия клавиши и интервалы между нажатиями, скорость набора текста (среднее количество нажатий клавиш за заданное время), наложение определенных комбинаций клавиш, соотношение использования клавиш «Shift» или «Capslock» для ввода прописных/строчных букв, количество ошибок, методы исправления ошибок, и использование клавиш навигации (со стрелками) для перемещения курсора. В [35] показано, что всего две характеристики и простой классификатор могут обеспечить достаточно эффективную идентификацию пользователя.

Нажатие клавиши генерирует три основных события: событие опускания клавиши, событие отпускания клавиши и событие нажатия клавиши (происходит при вставке символа в текст) [36]. Перечисленные события используются для извлечения характеристик, разделенных на две группы: глобальные и временные.

Глобальные характеристики описывают общее поведение пользователя при наборе текста, такое как частота ошибок, удаление символов, использование клавиш «Shift», «Control», «Alt», общая скорость набора текста (нажатия клавиш или слов в минуту).

Временны́е характеристики относятся к стилю нажатия определенных клавиш или их комбинаций, на основе которых могут быть извлечены значения времени между (рисунок 5) [37]:

– отпусканием одной клавиши и нажатием следующей;

– нажатием и отпусканием одной и той же клавиши;

– нажатием одной клавиши и отпусканием следующей;

– нажатиями одной и следующей клавиш;

– отпусканием одной и следующей клавиш.

Идентификация пользователей – не единственное применение динамики нажатия клавиш. Эти свойства также могут быть применены в целях профилирования пользователей. За последнее десятилетие методы распознавания на основе нажатий клавиш привлекают все большее внимание в качестве инструмента компьютерной криминалистки в поведенческой биометрии. Исследования в этой

области чаще всего сосредоточены на определении возраста и пола человека, но также в [38] была создана модель машинного обучения для оценки уровня образования. Хотя точность такой модели составляла более 85 %, это решение имело ряд ограничений, в том числе высокую вычислительную сложность, которая связана с длительным временем обучения модели.

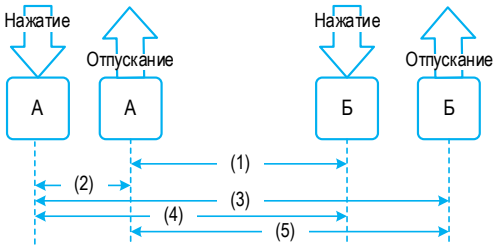

Рис. 5. Временны́е характеристики нажатия клавиш

Fig. 5. Time Characteristics of Key Presses

Тексты, используемые в экспериментах, могут иметь определенную длину (например, логин или пароль) или представлять собой спонтанное, ранее неопределенное содержание с неизвестным количеством букв. Первый вариант применяется в большинстве исследований, касающихся динамики нажатия клавиш. В настоящее время работы, проводимые в этой области, сосредоточены на усовершенствовании известных методов обработки временных характеристик [39–40]. Второй подход с нефиксированной длинной текста может быть использован для непрерывной идентификации. Этот подход исследуется как для стандартной клавиатуры, так и для смартфонов. В [41] авторы разработали Android-приложение IProfile для сбора событий нажатия клавиш на виртуальной клавиатуре. Во время эксперимента, в ходе которого участники набирали пароль, было извлечено 155 параметров. При этом точность различными методами классификации составила примерно 97 %.

2.1.2. Динамика движения курсора мыши и пальца

Другим примером поведенческой биометрии является динамика движения мыши, где идентификация пользователей осуществляется на основе того, как они используют свою мышь на компьютере. Поведенческий профиль создается путем извлечения характеристик, связанных с движениями мыши пользователя.

Ранние исследования динамики движения мыши были сосредоточены на распознавании электронных подписей пользователей. Например, в [42] использовали нейронные сети для изучения подписей, сделанных от руки. В 2003 г. в работе [43] проведено исследование подписывания с помощью мыши.

В 2007 г. в [44] представлено исследование возможности использования данных о перемещении мыши для идентификации личности. В предложенном подходе, актуальном и по сей день, выделяют следующие категории действия мыши:

– движение мыши;

– действие начинается с нажатия кнопки мыши, перемещения, а затем отпускания кнопки мыши;

– движение мыши, за которым следует щелчок или двойной щелчок;

– отсутствие движения.

Каждое такое действие состоит из следующих значений: пройденное расстояние в пикселях, прошедшее время в секундах и направление движения. Рассматриваются восемь направлений, охватывающих набор движений мыши в пределах 45 ° (рисунок 6).

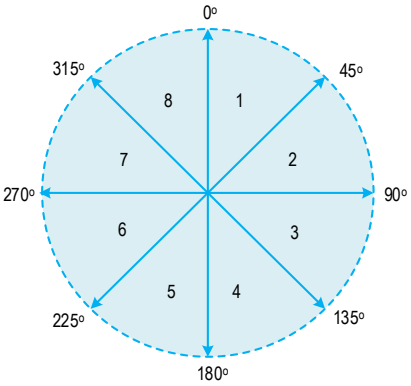

Рис. 6. Направления движения мыши

Fig. 6. Directions of Mouse Movement

Характеристики динамики мыши могут быть описаны набором параметров, полученных в результате анализа зафиксированных действий мыши. Эти параметры представляют собой составные части сигнатуры динамики мыши для конкретного пользователя, которая может быть использована для его идентификации. Среди них – средняя скорость движения каждого пройденного расстояния, движения в каждом направлении, среднее пройденное расстояние за определенный период времени по различным направлениям движения.

Аналогично динамике нажатия, современные мобильные устройства также привносят в динамику движения пальца по сенсору такие дополнительные параметры, как давление на экран и площадь экрана, на которую нажимает палец. Так, например, в [45] исследована точность жестов смахивания, используя продолжительность касания, длину траектории смахивания, среднюю скорость, ускорение, давление и площадь пальцев при движении. В рамках исследования было собрано 58 образцов от 40 испытуемых, и была проведена классификация, которая обеспечила уровень ошибок 0,004 %.

Также отмечается, что сенсорные данные зависят от приложений, поэтому не следует ожидать универсальной оценки эффективности для всех приложений, а вместо этого следует рассмотреть

варианты реализации в контексте конкретного приложения. Так, в [46] предлагается подход, суть которого заключается в исследовании преимуществ и недостатков идентификации на уровне устройств и приложений. Для эксперимента авторы разработали четыре приложения для 32 пользователей, которые использовали их в естественных условиях в течение десяти недель. Записывались характеристики сенсорного экрана, включая такие показатели, как координаты точки касания, давление пальца, площадь, ориентация экрана. В результате было отмечено, что показатели различаются в зависимости от приложения, следовательно, значимость характеристик различается в зависимости от приложения. Результаты экспериментов также показывают, что этот подход является более точным, чем подход, ориентированный на устройство, поскольку количество недостоверных признаков уменьшается.

2.1.3. Движение устройства

Мобильные устройства позволяют определять его движение с помощью встроенных акселерометров и гироскопов. Акселерометр измеряет ускорение в трех ортогональных пространственных измерениях: *x*, *y* и *z* [47]. Гироскоп измеряет вращение вокруг каждой из этих осей [48]. Комбинация этих измерений предоставляет пространство признаков, позволяющее моделировать движение пользователя.

Например, в [49] предлагается реализация, которая включает в себя так называемую воздушную подпись. Пока пользователь держит мобильное устройство в руках, он двигает его в воздухе, а измерения акселерометра записываются. Такая реализация требует от пользователя запуска приложения для сбора данных, поэтому она не является ни скрытой, ни прозрачной. Кроме того, сопоставление выполняется на сервере, что представляет угрозу безопасности в случае перехвата трафика. Тем не менее, алгоритм был протестирован на десяти добровольцах и показал 1,46 % ошибок 2 рода и 6,87 % ошибок 1 рода. В работе [50] предлагаются подобные попытки оценивания жестов махания, в [51] – жестов в свободной форме и в [52] – движения «поднятия руки» (т. е. доставания устройства из кармана, поднятия руки и поднесения телефона к уху).

Распознавание походки – это идентификация человека по тому, как он ходит, на основе методов машинного зрения, датчиков положения на полу или носимых датчиков. К последним можно отнести акселерометр и гироскоп мобильного устройства. Так, в [53] предлагается одна из таких систем идентификации пользователя, в которой продемонстрированно, как движения рук человека при ходьбе могут быть распознаны с помощью акселерометра и гироскопа в носимых устройствах. Для идентификации пользователя система применяет метод оценки и выбора признаков на основе корреляции, а также классификатор на основе скользящего окна. В результате авторы заявляют, что такая система отвечает ряду ключевых требований к идентификации пользователей по походке на устройствах с ограниченными ресурсами, таких как классификация в реальном времени, высокая точность идентификации и небольшое количество датчиков. Однако эта система ориентирована только на идентификацию по походке.

2.1.4. Голос

Метод на основе распознавания голоса объединяет физиологические и поведенческие характеристики для идентификации пользователя по его речи. Анатомические аспекты, например, голосовые связки, в сочетании с поведенческими характеристиками, такими как возраст или тональность, позволяют оценить множество характеристик, которые могут быть проанализированы статистически.

В [54] выделяется два способа распознавания голоса: текстозависимый и текстонезависимый. В первом случае пользователей просят произнести заранее определенную фразу, поэтому они знают о биометрической системе (следовательно, это не скрытая система). Из-за использования фиксированной фразы система работает точнее. Во втором – система пытается распознать говорящего независимо от того, что он произносит. Текстонезависимые системы полезны, когда существует меньший контроль над вводом, например, когда пользователь не знает о биометрической системе, что впоследствии обеспечивает большую гибкость. Однако, достижение высокой точности при распознавании голоса в такой системе является более сложной задачей из-за непредсказуемости говорящего.

Распознавание пользователя по особенностям голоса происходит по типичной схеме, начиная со сбора и предварительной обработки данных, извлечения и отбора характеристик и заканчивая моделированием и распознаванием образов. Как и в обычных системах на основе машинного обучения, качество характеристик вносит значительный вклад в точность идентификации пользователя. К таковым относятся краткосрочные спектральные, временные и ритмические, лингвистические характеристики, характеристики источника голоса и уровня разговора [55]. Краткосрочные спектральные характеристики представляют собой резонансные характеристики голосового тракта и часто извлекаются с высокой частотой для временны́х интервалов от 20 до 30 мс. Лингвистические и временные характеристики включают в себя интонационные и ритмические шаблоны, извлекаемые из длительных временных интервалов. Признаки разговорного уровня – это высокоуровневые свойства,

извлекаемые из текстового содержания устной речи, такие как частота слов или фраз. Качество характеристик измеряется их различительной способностью и устойчивостью к возможным внешним шумам (например, состояние пользователя и окружающая среда). Исследование [54] показало, что спектральные признаки обеспечивают высококачественное, простое и дискриминационное пространство признаков.

Последние достижения в области глубокого обучения привели к появлению инструментов синтеза требуемого голоса, которые создают синтетическую речь, произносимую голосом идентифицируемого пользователя, инструментов преобразования текста в речь, преобразующих произвольный текст в произносимые слова [56–57], а также инструментов, которые преобразуют существующие образцы голоса в тот же текст, который произносит идентифицируемый пользователь [58–60]. В [61] выделяют следующие методы синтеза голоса, позволяющие обойти системы идентификации на основе голоса: запись и воспроизведение [62–63], имитация голоса [64–65], машинный синтез (классический) [66–67], машинный синтез (на основе глубоких нейронных сетей) [68]. Для защиты систем распознавания речи от атак с использованием синтетической речи было предложено множество средств защиты. В то время как большинство из них сосредоточено на обнаружении синтетической речи [69–70], в [71] предлагается новое направление защиты – предотвращение несанкционированного синтеза голоса путем встраивания возмущений в аудиообразцы для их смещения в пространстве признаков.

2.1.5. Поведенческий профиль

Под поведенческим профилем понимаются интерактивные данные об использовании устройства, например, о том, как пользователь взаимодействует с мобильным устройством при совершении телефонных звонков, отправке текстовых сообщений и использовании приложений.

Работы в отношении интерактивных данных в основном связаны с обработкой нечисловых данных простым способом, например, с помощью подсчета частоты и категориальных представлений. В основном такой подход связан с невозможностью математической обработки этих значений. Значения интерактивных данных обычно представляют названия открытых или закрытых приложений или сетей Wi-Fi, к которым пользователь подключает устройство для доступа в Интернет [72].

Характеристики классифицируются следующим образом.

Категориальные: категориальные представления характеристик группируют интерактивные значения данных. Например, вместо того, чтобы перечислять названия каждого приложения для социальных сетей, вектор характеристик может просто включать само слово «социальная сеть» в качестве характеристики. Таким образом, если пользователь посещает пять социальных сетей, вектор характеристик будет указывать только на то, что приложения были для социальных сетей, не предоставляя точных сведений о них. В [73] рассмотрен этот подход для классификации трафика приложений. Время сбора данных группируется по времени суток, значения перемещения группируются по скорости, а значения местоположения устройства по наиболее частому и долгому пребыванию пользователя, например, на работе. Аналогично, в [74] классифицируется трафик приложений по таким группам, как музыка, обмен сообщениями и настройки. Очевидно, что такой подход сокращает значения характеристик до меньшего набора, который может быть слишком обобщенным, чтобы идентифицировать пользователей.

Частотные: представление характеристик на основе частоты основано на подсчете того, сколько раз выполняется то или иное действие [75]. Так, например, в [76] рассматривается частотное повторение действий для приложений и просмотра веб-страниц.

Последовательности: последовательности действий также являются характеристиками. В [77] предполагается, что порядок выполнения действий является значимым и уникальным для каждого пользователя. Этот подход похож на представление *n*-грамм для текста в приложениях стилометрии, где классификация основывается на частых *n*-кортежах, встречающихся в документах, идентифицируя стиль автора.

Для профилирования поведения были рассмотрены различные варианты реализации. Например, в [78] исследуется профилирование поведения как средство ассоциации условий с поведением. Пятьдесят студентов были привлечены к этому исследованию на один месяц, в течение которого записывались данные GPS, GSM, системные данные, журнал вызовов, данные датчиков и взаимодействия. Все добровольцы смогли подтвердить, что 95 % ассоциаций, обнаруженных исследователями, были верными.

Поведенческое профилирование также может использоваться для классификации вредоносных программ, так, в [79] предложено приложение Andro-prolifer как средство анализа системных вызовов, их аргументов и системных журналов для обнаружения вредоносных приложений на мобильных устройствах. В этой работе предпринята инновационная попытка устранить недостатки предыдущих подходов к обнаружению вредоносного программного обеспечения, которые в основном фокусировались на частоте системных вызовов, поскольку количество вызовов обычно невелико.

Авторы используют базу данных из 709 образцов вредоносного программного обеспечения и 350 доброкачественных образцов, достигая средней точности классификации 99 %. Наиболее значимые работы в области цифровых отпечатков пользователя приводятся в таблице 4.

ТАБЛИЦА 4. Основные исследования поведенческой биометрии

TABLE 4. Basic Research on Behavioral Biometrics

Ссылка	Год	Цитируемость	Описание	Параметры
[37]	2013	391	Представлен подробный обзор и сравнение исследований в области биометрии динамики нажатия клавиш.	• время между отпусканием одной клавиши и нажатием следующей; • время между нажатием и отпусканием одной и той же клавиши; • время между нажатием одной клавиши и отпусканием следующей; • время между нажатием одной и следующей клавиш; • время между отпусканием одной и следующей клавиш.
[44]	2007	480	Представлена новая форма поведенческой биометрии, основанная на динамике мыши, которая может быть использована в различных приложениях безопасности.	• средняя скорость движения; • средняя скорость движения в каждом направлении; • среднее пройденное расстояние за определенный период времени по различным направлениям движения.
[47]	2016	34	Исследования направлены на изучение возможности идентификации пользователей по значениям с датчиков акселерометра и гироскопа.	Координаты ускорения в трех ортогональных пространственных измерениях и вращения вокруг каждой из них.
[48]		17		
[54]	2002	933	Представлен краткий обзор методов распознавания речи, описывая применения, основные методы и некоторые показатели эффективности. Приведены методы синтетической речи и предотвращения несанкционированного синтеза голоса.	• краткосрочные спектральные характеристики; • временные и ритмические характеристики; • характеристики источника голоса; • лингвистические характеристики; • характеристики уровня разговора.
[55]	2016	632		
[69]	2020	49		
[70]	2019	58		
[71]	2021	28		
[57]	2013	22	В работах выделены разновидности интерактивных данных о поведении пользователей мобильных устройств.	• категориальные характеристики: тип приложения, время суток, скорость перемещения, местоположение; • частотные характеристики: частота запуска приложения, частота действий в приложении, частота просмотра веб-страниц; • характеристики последовательностей: порядок запуска приложений, порядок действия в приложении, последовательность символов в набираемом тексте.
[60]	2016	232		
[61]	2013	156		

2.2. Наборы данных

Существует множество наборов данных, однако многих из них нет в свободном доступе или содержат малое количество атрибутов. Поэтому для исследовательских целей стоит выделить 3 общедоступных крупномасштабных набора данных: UMDAA-02 [80], HuMIdb [81] и BehavePassDB [82]. В таблице 5 представлен краткий обзор этих трех исследований по поведенческой биометрии. Набор данных UMDAA-02 состоит из 141,14 ГБ сигналов датчиков смартфона, собранных у 48 добровольцев на телефонах Nexus 5 в течение двух месяцев [83]. К датчикам сбора данных относится фронтальная камера, сенсорный экран, гироскоп, акселерометр, магнитометр, датчик освещенности, GPS, Bluetooth, WiFi, датчики приближения, температуры и давления. Приложение для сбора данных также сохраняло время событий блокировки и разблокировки экрана, временные метки начала и окончания звонков, текущее открытое на экране приложение и т. д.

ТАБЛИЦА 5. Обзор исследований по поведенческой биометрии

TABLE 5. Overview of Behavioral Biometrics Studies

Объекты исследования	UMDAA-02 (2016), шт	HuMIdb (2020), шт	BehavePassDB (2022), шт
Сенсоры	10	14	15
Пользователи	48	600	81
Устройства	–	600	81

Набор данных Human Mobile Interaction (HuMIdb) включает более 5 ГБ данных для широкого спектра мобильных датчиков, полученных без сценария [84]. В базе данных хранятся данные от 14 датчиков

во время естественного взаимодействия человека с мобильным устройством, осуществляемого 600 пользователями. Для сбора данных было создано Android-приложение, которое собирает данные от датчиков во время выполнения пользователями 8 простых задач с помощью собственных мобильных устройств без какого-либо контроля (т. е. пользователи могли стоять, сидеть, ходить, находиться в помещении, на улице, днем или ночью и т. д.). Участники для эксперимента были отобраны по всему миру, что позволило получить более разнообразных участников, чем в предыдущих исследованиях.

BehavePassDB включает данные, также полученные во время естественного взаимодействия человека с мобильным устройством [85]. Сбор данных проводился в течение четырех сессий, каждая из которых была разделена по крайней мере 24-часовым промежутком. Испытуемых просили установить Android-приложение на свой смартфон и выполнить восемь заданий в неконтролируемом сценарии. Процесс сбора данных был разработан таким образом, чтобы имитировать наиболее важные сценарии взаимодействия человека и устройства в рамках прозрачной непрерывной аутентификации, т. е. поведенческие биометрические характеристики пользователя постоянно проверяются в течение всего времени использования устройства, не прерывая процесса идентификации. Кроме того, сессии сбора данных сбыли структурированы таким образом, чтобы сбалансировать количество собираемой информации и легкость сбора, чтобы вовлечь большое количество пользователей.

В таблице 6 приведена сводка атрибутов, собираемых в исследованиях по поведенческой биометрии.

ТАБЛИЦА 6. Информации и ее источник в исследованиях по поведенческой биометрии

TABLE 6. Information and Its Source in Behavioral Biometrics Research

Источник информации	UMDAA-02	HuMIdb	BehavePassDB
	Информация		
Акселерометр	*x, y, z*	*x, y, z*	*x, y, z*
Гироскоп	*x, y, z*	*x, y, z*	*x, y, z*
Сенсор гравитации	*x, y, z*	Значение ускорения	*x, y, z*
Датчик освещенности	Значение освещенности	Значение освещенности	Значение освещенности
Линейный акселерометр	*x, y, z*	*x, y, z*	*x, y, z*
Магнитометр	*x, y, z*	*x, y, z*	*x, y, z*
Касание экрана	*x, y*, давление, тип действия	*x, y*, давление, тип действия	*x, y*, тип действия
Разрешение экрана	*x, y*	–	–
Нажатие клавиши	ASCII-код, давление, тип	ASCII-код, давление	ASCII-код
Ориентация устройства	–	Значение ориентации (альбомная или книжная)	Значение ориентации (альбомная или книжная)
Датчик давления	–	–	Значение давления
Датчик приближения	–	Уровень приближения	Уровень приближения
GPS	Широта, долгота, точность	Широта, долгота, высота, пеленг, точность	Широта, долгота, высота, пеленг, точность
Wi-Fi	SSID, BSSID, тип аутентификации, IP-адрес, RSSI	SSID, уровень сигнала, информация о соединении, канал, частота	SSID, уровень сигнала, информация о соединении, канал, частота
Bluetooth	Производитель, флаг сопряжения	SSID, MAC-адрес	SSID, MAC-адрес
Датчик температуры	Значение температуры	Значение температуры	Значение температуры
Батарея	–	–	Уровень заряда
Датчик влажности	–	Уровень влажности	Уровень влажности
Микрофон	–	Аудиосигнал	–
Потребляемые ресурсы	Проценты загрузки процессора и ОЗУ	–	–
Приложение	Время запуска, продолжительность, время завершения, название приложения, флаг запуска с главного экрана	–	–

2.3. Применение цифровых отпечатков пользователя

В большинстве существующих компьютерных систем после авторизации ее ресурсы доступны пользователю до тех пор, пока он не выйдет из системы или не заблокирует сеанс. Фактически, в этот период ресурсы системы доступны любому пользователю. Например, идентификация на веб-ресурсе на основе цифрового отпечатка браузера. Однако это может привести к перехвату сеанса, когда злоумышленник нацеливается на открытый сеанс. В системах с высоким уровнем риска непрерывная идентификация личности пользователя чрезвычайно важна. Поведенческая биометрия позволяет осуществлять постоянное наблюдение за пользователями по его динамическим параметрам, например, таким как динамика нажатия [86] или динамика движения [87]. Она позволяет убедиться, что системой пользуется только авторизованный пользователь, даже после того, как была проведена первичная проверка личности. На сегодняшний день представлено множество реализаций непрерывной аутентификации от разных компаний.

Основанная в 2016 г. компания Plurilock работает над системой аутентификации с использованием поведенческой биометрии [86]. В разработанных продуктах Plurilock Aware и Plurilock Defend используется концепция жестов для аутентификации пользователей на основе динамики нажатия клавиш и движения мыши. Plurilock Aware решает проблему ввода учетных данных и избавляет от необходимости набирать пароли. Программа обеспечивает проверку личности путем распознавания шаблонов набора текста пользователей. Plurilock Defend обнаруживает легитимного пользователя, пока сессия активна, используя непрерывную аутентификацию. Если с помощью непрерывного отслеживания нажатия клавиш и мыши выявляется риск, то система получается оповещение. Эти продукты используют запатентованные алгоритмы для обеспечения непрерывной аутентификации в высокорегулируемых средах, таких как государственные учреждения, критически важные объекты инфраструктуры, финансовые услуги и здравоохранение.

Компания ThreatMark предоставляет полный пакет услуг по предотвращению текущего и будущего цифрового мошенничества [87]. ThreatMark работает над подготовкой решений для банков по борьбе с мошенничеством, начиная с раннего обнаружения угроз, поведенческой биометрии и заканчивая анализом риска транзакций.

Система идентификации голоса, разработанная компанией Aculab, захватывает десятки тысяч уникальных голосов и речевых характеристик для авторизации пользователя в режиме реального времени [88]. Утверждается, что их продукт является идеальной системой для голосовой биометрической системы аутентификации с точки зрения производительности и точности.

Система анализа поведения пользователей Cynet постоянно отслеживает и составляет профиль их активности [89]. Этот профиль впоследствии используется для определения базовой модели легитимного поведения и выявления аномальной активности, свидетельствующей о компрометации учетных записей. Система обеспечивает отслеживание всех взаимодействий в реальном времени с момента, когда пользователи начинают вход в систему.

UnifyID разработали платформу пассивной поведенческой аутентификации, предназначенной для идентификации пользователей без каких-либо осознанных действий со их стороны [90]. Разработанная платформа использует методы машинного обучения для обеспечения повышенной точности при улучшении пользовательского опыта.

SecureTouch работает над созданием технологий непрерывной аутентификации для укрепления безопасности и снижения уровня мошенничества при одновременном улучшении цифрового опыта клиентов на мобильных устройствах [91]. Их системы собирают и анализируют более чем 100 различных поведенческих параметров, таких как динамика нажатий, скорость прокрутки, давление при нажатии на экран и размер пальцев, чтобы автоматически создать уникальный поведенческий профиль пользователя, который впоследствии может быть использован для аутентификации.

Заключение

Одной из базовых задач обеспечения информационной безопасности является идентификация и аутентификация субъектов информационных процессов, в том числе протекающих в такой среде как Интернет и реализуемых с помощью коммуникационных средств Интернет-ресурсов (веб-сайтов, социальных сетей, форумов). Идентификация является основой систем разграничения доступа, и, в том числе, к Интернет-ресурсам или отдельным сервисам.

На сегодняшний день существуют две основные группы методов идентификации пользователя: по техническим характеристикам рабочей станции пользователя и по поведенческим характеристикам пользователя компьютерной системы.

Первая группа методов является хорошо проработанной и наиболее распространенной. Идентификация производится по характеристикам аппаратного и программного окружения рабочей станции пользователя, с которой осуществляется доступ ресурсу, например, через браузер. К достоинствам первой

группы методов можно отнести достаточно высокую точность идентификации, однако она обладает одним существенным недостатком: производится идентификация рабочей станции, с которой осуществляется доступ, а не конкретного пользователя этот доступ осуществляющего.

Одним из наиболее перспективных направлений развития технологий идентификации является поведенческая идентификация. Данные методы основываются на поведении пользователя. Каждый человек имеет свое уникальное поведение, которые составляют своеобразный уникальный цифровой отпечаток – набор характеристик, позволяющих его идентифицировать. Применение данного подхода позволяет произвести идентификации пользователя, а не его рабочей станции. Однако эти методы обладают несколькими недостатками и ограничениями: поведенческие характеристики пользователя обладает достаточно низкой различающей способностью.

Список источников

1. Агафонов Ю.М. Деанонимизация пользователей на основе цифровых отпечатков браузера // XVI Всероссийская научно-практическая конференция студентов, аспирантов, молодых ученых «Безопасность информационного пространства – 2017» (Екатеринбург, Российская Федерация, 12 декабря 2017). Екатеринбург: Изд-во Урал. ун-та, 2018. С. 3–5.
2. Алисултанова Э.Д., Исаева М.З., Болтиев Д.У. Анализ систем автономной идентификации пользователя сайта // Электронная наука. 2021. Т. 2. № 2. С. 7.
3. Ишкуватов С.М., Комаров И.И. Анализ аутентичности трафика на основании данных цифровых отпечатков реализаций сетевых протоколов // Научно-технический вестник информационных технологий, механики и оптики. 2020. Т. 20. № 5. С. 747–754. DOI:10.17586/2226-1494-2020-20-5-747-754
4. Балмаев И.Т. Идентификация пользователей сети Tor на основе параметров перехваченного трафика // Межвузовская научно-техническая конференция студентов, аспирантов и молодых специалистов им. Е.В. Арменского (Москва, Российская Федерация, 17 февраля – 01 марта 2017). Москва: Московский институт электроники и математики НИУ ВШЭ, 2017. С. 372–373.
5. Шулицкий Д.С., Водейко А.Э. Методы защиты авторского права на программные продукты с помощью водяных знаков и отпечатков пальцев. 2019. URL: https://libeldoc.bsuir.by/bitstream/123456789/37230/1/Shulitskiy_Metody.pdf (дата обращения 20.10.2023)
6. Гусев П.Д. Обзор существующих алгоритмов построения цифровых отпечатков // Безопасность информационных технологий. 2015. Т. 22. № 4. С. 63–67.
7. Борисова С.Н. Методы защиты аудиофайлов от несанкционированного копирования и распространения // Фундаментальные исследования. 2015. № 5-3. С. 481–487.
8. Eckersley P. How Unique Is Your Web Browser? // Proceedings of the 10th International Symposium on Privacy Enhancing Technologies Symposium (PETS 2010, Berlin, Germany, 21–23 July 2010). Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2010. Vol. 6205. PP. 1–18. DOI:10.1007/978-3-642-14527-8_1
9. Mowery K., Shacham H. Pixel Perfect: Fingerprinting Canvas in HTML5 // Proceedings of W2SP. 2012. URL: https://api.semanticscholar.org/CorpusID:1399943 (Accessed 20.10.2023)
10. Cao Y., Li S., Wijmans E. (Cross-) Browser Fingerprinting via OS and Hardware Level Features // NDSS' 2017 (26 February – 1 March 2017, San Diego, USA). 2017. DOI:10.14722/ndss.2017.23152
11. Englehardt S., Narayanan A. Online tracking: A 1-million-site Measurement and Analysis // Proceedings of the Conference on Computer and Communications Security (2016 ACM SIGSAC, Vienna, Austria, 24–28 October 2016). New York: Association for Computing Machinery, 2016. PP. 1388–1401. DOI:10.1145/2976749.2978313
12. Sjösten A., Van Acker S., Sabelfeld A. Discovering Browser Extensions via Web Accessible Resources // Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy (CODASPY '17, Scottsdale, USA, 22–24 March 2017). New York: Association for Computing Machinery, 2017. PP. 329–336. DOI:10.1145/3029806.3029820
13. Sanchez-Rola I., Santos I., Balzarotti D. Extension Breakdown: Security Analysis of Browsers Extension Resources Control Policies // Proceedings of the 26th USENIX Conference on Security Symposium (USENIX Security 17, Vancouver, Canada, 16–18 August 2017). Berkeley: USENIX Association, 2017. PP. 679–694.
14. Starov O., Nikiforakis N. Xhound: Quantifying the Fingerprintability of Browser Extensions // Proceedings of the Symposium on Security and Privacy (SP, San Jose, USA, 22–26 May 2017). IEEE, 2017. PP. 941–956. DOI:10.1109/SP.2017.18
15. Mowery K., Bogenreif D., Yilek S., Shacham H. Fingerprinting Information in JavaScript Implementations. 2012. URL: https://search.iczhiku.com/paper/hgdOSDNQ7g2K8zv8.pdf (Accessed 20.10.2023)
16. Nakibly G., Shelef G., Yudilevich S. Hardware Fingerprinting Using HTML5 // arXiv:1503.01408. 2015. DOI:10.48550/arXiv.1503.01408
17. Olejnik Ł., Acar G., Castelluccia C., Diaz C. The leaking battery // Proceedings of the International Workshop on Data Privacy Management International Workshop on Quantitative Aspects in Security Assurance. 2015. С. 254–263. DOI:10.1007/978-3-319-29883-2_18
18. Vastel A., Laperdrix P., Rudametkin W., Rouvoy R. FP-STALKER: Tracking Browser Fingerprint Evolutions // Proceedings of the Symposium on Security and Privacy (SP, San Francisco, USA, 20–24 May 2018). IEEE, 2018. PP. 728–741. DOI:10.1109/SP.2018.00008
19. Laperdrix P., Rudametkin W., Baudry B. Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints // Proceedings of the Symposium on Security and Privacy (SP, San Jose, USA, 22–26 May 2016). IEEE, 2016. PP. 878–894. DOI:10.1109/SP.2016.57

20. Gómez-Boix A., Laperdrix P., Baudry B. Hiding in the Crowd: an Analysis of the Effectiveness of Browser Fingerprinting at Large Scale // Proceedings of the World Wide Web Conference (Lyon, France, 23–27 April 2018). 2018. PP. 309–318. DOI:10.1145/3178876.3186097
21. A look into several Angler Exploit Kit malvertising campaigns // Operation Fingerprint. 2016. URL: https://malware bytes.app.box.com/v/operation-fingerprint (дата обращения 26.04.2023)
22. ThreatMetrix – Cybersecurity Risk Management // LexisNexis Risk Solutions. URL: https://risk.lexisnexis.com/products/ threatmetrix (дата обращения 26.04.2023)
23. The Evolution of Hi-Def Fingerprinting in Bot Mitigation // Imperva. 2018. URL: https://www.imperva.com/blog/the-evolution-of-hi-def-fingerprinting-in-bot-mitigation (дата обращения 26.04.2023)
24. Track Devices // MaxMind. 2023. URL: https://dev.maxmind.com/minfraud/track-devices (дата обращения 26.04.2023)
25. Safeguard Websites, Mobile Apps & APIs From Bots // HUMAN Bot Defender. 2023. URL: https://www.humansecurity. com/products/human-bot-defender#scroll-down (дата обращения 26.04.2023)
26. Device Fingerprint // IPQualityScore. 2023. URL: https://www.ipqualityscore.com/device-fingerprinting (дата обращения 26.04.2023)
27. Comprehensive Bot Management // Radware. 2023. URL: https://www.radware.com/products/bot-manager (дата обращения 26.04.2023)
28. Fraud Detection Software for Secure Growth // Sift. 2023. URL: https://sift.com/products/digital-trust-safety-platform (дата обращения 26.04.2023)
29. Device Recognition // SecurAuth. 2023. URL: https://docs.secureauth.com/2104/en/device-recognition.html (дата обращения 26.04.2023)
30. TruValidate // TransUnion. 2023. URL: https://www.transunion.com/solution/truvalidate (дата обращения 26.04.2023)
31. Murashko Yu.V., Papaev B.N. Increasing the accuracy of user identification by digital fingerprint using a two-stage approach // X International Scientific and Practical Conference "Prospective scientific research: experience, problems and prospects of development". 2023. С. 191-195.
32. Murashko Yu.V. Идентификация пользователей в сетевом трафике // Всероссийская научно-техническая конференция «Актуальные проблемы радиоэлектроники и телекоммуникаций» (Самара, Российская Федерация, 25–28 апреля 2023). 2023. С. 166–169.
33. Sultana M., Paul P.P., Gavrilova M. A Concept of Social Behavioral Biometrics: Motivation, Current Developments, and Future Trends // Proceedings of the International Conference on Cyberworlds (Santander, Spain, 06–08 October 2014). IEEE, 2014. PP. 271–278. DOI:10.1109/CW.2014.44
34. Мурашко Ю.В. Идентификация пользователей сети по их поведению // IX Всероссийская научно-техническая конференция «Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности» (Таганрог, Российская Федерация, 10–15 апреля 2023). Ростов-на-Дону: Южный федеральный университет, 2023. С. 54–56.
35. Rybnik M., Tabedzki M., Adamski M., Saeed K. An Exploration of Keystroke Dynamics Authentication Using Non-fixed Text of Various Length // Proceedings of the International Conference on Biometrics and Kansei Engineering (Tokyo, Japan, 05–07 July 2013). IEEE, 2013. PP. 245–250. DOI:10.1109/ICBAKE.2013.48
36. Shimshon T., Moskovitch R., Rokach L., Elovici Y. Continuous Verification Using Keystroke Dynamics // Proceedings of the International Conference on Computational Intelligence and Security (Nanning, China, 11–14 December 2010). IEEE, 2010. PP. 411–415. DOI:10.1109/CIS.2010.95
37. Teh P.S., Teoh A.B.J., Yue S. A Survey of Keystroke Dynamics Biometrics // The Scientific World Journal. 2013. Vol. 2013. P. 408280. DOI:10.1155/2013/408280
38. Tsimperidis I., Yoo P.D., Taha K., Mylonas A., Katos V. R²BN: An adaptive Model for Keystroke-Dynamics-Based Educational Level Classification // IEEE Transactions on Cybernetics. 2018. Vol. 50. Iss. 2. PP. 525–535. DOI:10.1109/TCYB.2018. 2869658
39. Alshanketi F., Traore I., Ahmed A.A. Improving Performance and Usability in Mobile Keystroke Dynamic Biometric Authentication // Proceedings of the IEEE Security and Privacy Workshops (SPW, San Jose, USA, 22–26 May 2016). IEEE, 2016. С. 66–73. DOI:10.1109/SPW.2016.12
40. Ali M.L., Thakur K., Tappert C.C., Qiu M. Keystroke Biometric User Verification Using Hidden Markov Model // Proceedings of the 3rd International Conference on Cyber Security and Cloud Computing (CSCloud, Beijing, China, 25–27 June 2016). IEEE, 2016. PP. 204–209. DOI:10.1109/CSCloud.2016.23
41. Krishnamoorthy S., Rueda L., Saad S., Elmiligi H. Identification of User Behavioral Biometrics for Authentication Using Keystroke Dynamics and Machine Learning // Proceedings of the 2nd International Conference on Biometric Engineering and Applications (ICBEA '18, Amsterdam, Netherlands, 16–18 May 2018). New York: Association for Computing Machinery, 2018. PP. 50–57. DOI:10.1145/3230820.3230829
42. Higashino J. Signature Verification System on Neuro-Computer // Proceedings of the 11th International Conference on Pattern Recognition (IAPR, Hague, Netherlands, 30 August – 3 September 1992). Vol. 3. 1992. PP. 517–521.
43. Everitt R.A.J., McOwan P.W. Java-based internet biometric authentication system // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2003. Vol. 25. Iss. 9. PP. 1166–1172. DOI:10.1109/TPAMI.2003.1227991
44. Ahmed A.A.E., Traore I. A New Biometric Technology Based on Mouse Dynamics // IEEE Transactions on Dependable and Secure Computing. 2007. Vol. 4. Iss. 3. PP. 165–179. DOI:10.1109/TDSC.2007.70207
45. Antal M., Szabó L.Z. Biometric Authentication Based on Touchscreen Swipe Patterns // Procedia Technology. 2016. Vol. 22. PP. 862–869. DOI:10.1016/j.protcy.2016.01.061

46. Khan H., Hengartner U. Towards application-centric implicit authentication on smartphones // Proceedings of the 15th Workshop on Mobile Computing Systems and Applications (Santa Barbara, USA, 26–27 February 2014). New York: Association for Computing Machinery, 2014. P. 10. PP. 1–6. DOI:10.1145/2565585.2565590

47. Ferrero R., Gandino F., Montrucchio B., Rebaudengo M., Velasco A., Benkhelifa I. On gait recognition with smartphone accelerometer // Proceedings of the 4th Mediterranean Conference on Embedded Computing (MECO, Budva, Montenegro, 14–18 June 2015). IEEE, 2015. PP. 368–373. DOI:10.1109/MECO.2015.7181946

48. Fantana A.L., Ramachandran S., Schunck C.H., Talamo M. Movement based biometric authentication with smartphones // Proceedings of the International Carnahan Conference on Security Technology (ICCST, Taipei, Taiwan, 21–24 September 2015). IEEE, 2015. PP. 235–239. DOI:10.1109/CCST.2015.7389688

49. Laghari A., Waheed-ur-Rehman, Memon Z.A. Biometric authentication technique using smartphone sensor // Proceedings of the 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST, Islamabad, Pakistan, 12–16 January 2016). IEEE, 2016. PP. 381–384. DOI:10.1109/IBCAST.2016.7429906

50. Hong F., Wei M., You S., Feng Y., Guo Z. Waving authentication: your smartphone authenticate you on motion gesture // Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (Seoul, Republic of Korea, 18–23 April 2015). New York: Association for Computing Machinery, 2015. PP. 263–266. DOI:10.1145/2702613.2725444

51. Ehatisham-ul-Haq M., Azam M.A., Naeem U., Amin Y., Loo J. Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing // Journal of Network and Computer Applications. 2018. Vol. 109. PP. 24–35. DOI:10.1016/j.jnca.2018.02.020

52. Feng T., Zhao X., Shi W. Investigating Mobile Device Picking-up motion as a novel biometric modality // Sixth International Conference on Biometrics on Theory, Applications and Systems (BTAS, Arlington, USA, 29 September – 02 October 2013). IEEE, 2013. DOI:10.1109/BTAS.2013.6712701

53. Oak R., Khare M. A Novel Architecture for Continuous Authentication Using Behavioural Biometrics // Proceedings of the International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC, Mysore, India, 8–9 September 2017). 2017. PP. 767–771. DOI:10.1109/CTCEEC.2017.8455040

54. Reynolds D.A. An Overview of Automatic Speaker Recognition Technology // Proceedings of the International Conference on Acoustics, Speech, and Signal Processing (ICASSP, Orlando, USA, 13–17 May 2002). IEEE, 2002. Vol. 4. PP. 4072–4075.

55. Ravanelli M., Bengio Y. Speaker Recognition from Raw Waveform with SincNet // Proceedings of the Spoken Language Technology Workshop (SLT, Athens, Greece, 18–21 December 2018). IEEE, 2018. PP. 1021–1028. DOI:10.1109/SLT.2018.8639585

56. Arik S., Chen J., Peng K., Ping W., Zhou Y. Neural Voice Cloning with a Few Samples // Proceedings of the 32nd Conference on Neural Information Processing Systems (NeurIPS 2018, Montréal, Canada, 3–8 December 2018). 2018. Vol. 31.

57. Hu Q., Marchi E., Winarsky D., Stylianou Y., Naik D., Kajarekar S. Neural Text-to-Speech Adaptation from Low Quality Public Recordings // Proceedings of the 10th ISCA Workshop on Speech Synthesis (SSW 10, Vienna, Austria, 20–22 September 2019). 2019. Vol. 10. PP. 24–28. DOI:10.21437/SSW.2019-5

58. Kameoka H. Stargan-vc: Non-parallel many-to-many voice conversion using star generative adversarial networks // Proceedings of the Spoken Language Technology Workshop (SLT, Athens, Greece, 18–21 December 2018). IEEE, 2018. PP. 266–273. DOI:10.1109/SLT.2018.8639535

59. Rebryk Y., Beliaev S. Convoice: Real-Time Zero-Shot Voice Style Transfer with Convolutional Network // arXiv:2005.07815. 2020. DOI:10.48550/arXiv.2005.07815

60. Wu D.Y., Chen Y.H., Lee H.Y. Vqvc+: One-Shot Voice Conversion by Vector Quantization and U-Net Architecture // arXiv:2006.04154. 2020. DOI:10.48550/arXiv.2006.04154

61. Wenger E., Bronckers M., Cianfarani C., Cryan J., Sha A., Zheng H., et al. "Hello, It's Me": Deep Learning-based Speech Synthesis Attacks in the Real World // Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (Virtual Event Republic of Korea, 15–19 November 2021). New York: Association for Computing Machinery, 2021. PP. 235–251. DOI:10.1145/3460120.3484742

62. Janicki A., Alegre F., Evans N. An assessment of automatic speaker verification vulnerabilities to replay spoofing attacks // Security and Communication Networks. 2016. Vol. 9. Iss. 15. PP. 3030–3044. DOI:10.1002/sec.1499

63. Kinnunen T., Sahidullah M., Delgado H., Todisco M., Evans N. Yamagishi J., et al. The ASVspoof 2017 Challenge: Assessing the Limits of Replay Spoofing Attack Detection. 2017. URL: https://www.eurecom.fr/~evans/papers/pdfs/5235.pdf (дата обращения 22.10.2023)

64. Gao Y., Lian J., Raj B., Singh R. Detection and Evaluation of Human and Machine Generated Speech in Spoofing Attacks on Automatic Speaker Verification Systems // Proceedings of the Spoken Language Technology Workshop (SLT, Shenzhen, China, 19–22 January 2021). IEEE, 2021. PP. 544–551. DOI:10.1109/SLT48900.2021.9383558

65. Vestman V., Kinnunen T., Hautamäki R.G., Sahidullah Md. Voice Mimicry Attacks Assisted by Automatic Speaker Verification // Computer Speech & Language. 2020. Vol. 59. PP. 36–54. DOI:10.1016/j.csl.2019.05.005

66. Masuko T., Hitotsumatsu T., Tokuda K., Kobayashi T. On the security of HMM-based speaker verification systems against imposture using synthetic speech // Proceedings of the Sixth European Conference on Speech Communication and Technology (EUROSPEECH 1999, Budapest, Hungary, 5-9 September 1999). 1999.

67. Mukhopadhyay D., Shirvanian M., Saxena N. All Your Voices are Belong to Us: Stealing Voices to Fool Humans and Machines // Proceedings of the 20th European Symposium on Research in Computer Security (ESORICS 2015, Vienna, Austria, 21–25 September 2015). Lecture Notes in Computer Science. Cham: Springer, 2015. Vol. 9327. PP. 599–621. DOI:10.1007/978-3-319-24177-7_30

68. Partila P., Tovarek J., Ilk G.H., Rozhon J., Voznak M. Deep Learning Serves Voice Cloning: How Vulnerable Are Automatic Speaker Verification Systems to Spoofing Trials? // IEEE Communications Magazine. 2020. Vol. 58. Iss. 2. PP. 100–105. DOI:10.1109/MCOM.001.1900396

69. Ahmed M.E., Kwak I.Y., Huh J.H., Kim I., Oh T., Kim H. Void: A fast and light voice liveness detection system // Proceedings of the 29th USENIX Security Symposium (USENIX Security, 12–14 August 2020). 2020. PP. 2685–2702.
70. AlBadawy E.A., Lyu S., Farid H. Detecting AI-Synthesized Speech Using Bispectral Analysis // Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops. 2019. PP. 104–109.
71. Huang C., Lin Y.Y., Lee H., Lee L. et al. Defending Your Voice: Adversarial Attack on Voice Conversion // Proceedings of the Spoken Language Technology Workshop (SLT, Shenzhen, China, 19–22 January 2021). IEEE, 2021. PP. 552–559. DOI:10.1109/SLT48900.2021.9383529
72. Kobayashi R., Yamaguchi R.S. A Behavior Authentication Method Using Wi-Fi BSSIDs around Smartphone Carried by a User // Proceedings of the Third International Symposium on Computing and Networking (CANDAR, Sapporo, Japan, 08–11 December 2015). IEEE, 2015. PP. 463–469. DOI:10.1109/CANDAR.2015.45
73. Bassu D., Cochinwala M., Jain A. A new mobile biometric based upon usage context // Proceedings of the International Conference on Technologies for Homeland Security (HST, Waltham, USA, 12–14 November 2013). IEEE, 2013. PP. 441–446. DOI:10.1109/THS.2013.6699045
74. Branscomb A.S. Behaviorally Identifying Smartphone Users. Master's Thesis. Raleigh: North Carolina State University, 2013.
75. Neal T.J., Woodard D.L., Striegel A.D. Mobile device application, Bluetooth, and Wi-Fi usage data as behavioral biometric traits // Proceedings of the 7th International Conference on Biometrics Theory, Applications and Systems (BTAS, Arlington, USA, 08–11 September 2015). IEEE, 2015. PP. 1–6. DOI:10.1109/BTAS.2015.7358777
76. Fridman L., Weber S., Greenstadt R., Kam M. Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location // IEEE Systems Journal. 2016. Vol. 11. Iss. 2. PP. 513–521. DOI:10.1109/JSYST.2015.2472579
77. Brocardo M.L., Traore I., Saad S., Woungang I. Authorship verification for short messages using stylometry // Proceedings of the International Conference on Computer, Information and Telecommunication Systems (CITS, Athens, Greece, 07–08 May 2013. IEEE, 2013. PP. 1–6. DOI:10.1109/CITS.2013.6705711
78. Cao H., Bao T., Yang Q., Chen E. An effective approach for mining mobile user habits // Proceedings of the 19th ACM International Conference on Information and Knowledge Management (CIKM 2010, Toronto, Canada, 26–30 October 2010). New York: Association for Computing Machinery, 2010. PP. 1677–1680. DOI:10.1145/1871437.1871702
79. Jang J., Yun J., Woo J., Kim H.K. Andro-profiler: anti-malware system based on behavior profiling of mobile malware // Proceedings of the 23rd International Conference on World Wide Web (WWW '14 Companion, Seoul, Korea, 7–11 April 2014). New York: Association for Computing Machinery, 2014. PP. 737–738. DOI:10.1145/2567948.2579366
80. UMDAA-02 Dataset // Github. 2018. URL: https://umdaa02.github.io (дата обращения 26.04.2023)
81. BiDAlab/HuMIdb // Github. 2020. URL: https://github.com/BiDAlab/HuMIdb (дата обращения 26.04.2023)
82. BiDAlab/MobileB2C_BehavePassDB // Github. 2022. URL: https://github.com/BiDAlab/MobileB2C_BehavePassDB (дата обращения 26.04.2023)
83. Mahbub U., Sarkar S., Patel V.M., Chellappa R. Active user authentication for smartphones: A challenge data set and benchmark results // Proceedings of the 8th international conference on biometrics theory, applications and systems (BTAS, Niagara Falls, USA, 06–09 September 2016). IEEE, 2016. PP. 1–8. DOI:10.1109/BTAS.2016.7791155
84. Acien A., Morales A., Fierrez J., Vera-Rodriguez R., Delgado-Mohatar O. BeCAPTCHA: Behavioral bot detection using touchscreen and mobile sensors benchmarked on HuMIdb // Engineering Applications of Artificial Intelligence. 2021. Vol. 98. P. 104058. DOI:10.1016/j.engappai.2020.104058
85. Stragapede G., Vera-Rodriguez R., Tolosana R., Morales A. BehavePassDB: Public Database for Mobile Behavioral Biometrics and Benchmark Evaluation // Pattern Recognition. 2023. Vol. 134. P. 109089. DOI:10.1016/j.patcog.2022.109089
86. Ananya S.S. Keystroke Dynamics for Continuous Authentication // Proceedings of the 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence, Noida, 11–12 January 2018). IEEE, 2018. PP. 205–208. DOI:10.1109/CONFLUENCE.2018.8442703
87. Mondal S., Bours P. Continuous authentication using mouse dynamics // Proceedings of the International Conference of the BIOSIG Special Interest Group (BIOSIG, Darmstadt, Germany, 05–06 September 2013). IEEE, 2013. PP. 1–12.
88. Plurilock AI – Least privilege CASB, DLP with DEFEND technology // Plurilock. 2016. URL: https://plurilock.com (дата обращения 26.04.2023)
89. ThreatMark Fraud Prevention Solution // ThreatMark. 2015. URL: https://www.threatmark.com (дата обращения 26.04.2023)
90. VoiSentry // Aculab. 2018. URL: https://www.aculab.com/biometric-technologies/voisentry (дата обращения 26.04.2023)
91. User Behavior Analytics (UBA) // Cynet. 2018. URL: https://www.cynet.com/platform/user-behaviour-analytics (дата обращения 26.04.2023)
92. Authentication platform // UnifyID. 2015. URL: https://unify.id (дата обращения 26.04.2023)
93. SecuredTouch Company Profile – Office Locations, Competitors, Financials, Employees, Key People, News // Craft.co. 2016. URL: https://craft.co/securedtouch (дата обращения 26.04.2023)

References

1. Agafonov Yu.M. Deanonymization of users based on digital fingerprints of the browser. *Proceedings of the XVI All-Russian Scientific and Practical Conference of Students, Graduate Students, Young Scientists on Security of the Information Space – 2017, 12 December 2017, Ekaterinburg, Russian Federation.* Ekaterinburg: Ural Federal University Publ.; 2018. p.3–5.
2. Alisultanova E.D., Isaeva M.Z., Baltiev D.U. Analysis of Systemsautonomous Site User Identification. *Elektronnaya nauka.* 2021;2(2):7.

3. Ishkuvatov S.M., Komarov I.I. Traffic Authenticity Analysis Based on Digital Fingerprint Data of Network Protocol Implementations. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics.* 2020:20(5):747–754. DOI:10.17586/2226-1494-2020-20-5-747-754

4. Balmaev I.T. Identification of Tor network users based on intercepted traffic parameters. *Proceedings of the Interuniversity Scientific and Technical Conference of Students, Postgraduates and Young Specialists, 17 February – 01 March 2017, Moscow, Russian Federation*. Moscow: Moscow Institute of Electronics and Mathematics, National Research University Higher School of Economics Publ.; 2017. p.372–373.

5. Shulitsky D.S., Vodeyko A E. *Methods of Copyright Protection for Software Products Using Watermarks and Fingerprints*. 2019. URL: https://libeldoc.bsuir.by/bitstream/123456789/37230/1/Shulitskiy_Metody.pdf [Accessed 20.10.2023]

6. Gusev P.D. Review of Existing Algorithms for Constructing Digital Fingerprints. *IT Security(Russia)*. 2015;22(4):63–67.

7. Borisova S.N. Methods of Protection from the Audio-Files from Unauthorized Copying and Distribution. *Fundamental research.* 2015;3-5:481–487.

8. Eckersley P. How Unique Is Your Web Browser? *Proceedings of the 10th International Symposium on Privacy Enhancing Technologies Symposium, PETS 2010, 21–23 July 2010, Berlin, Germany. Lecture Notes in Computer Science, vol.6205*. Berlin, Heidelberg: Springer; 2010. p.1–18. DOI:10.1007/978-3-642-14527-8_1

9. Mowery K., Shacham H. Pixel Perfect: Fingerprinting Canvas in HTML5. *Proceedings of W2SP*. 2012. URL: https://api.semanticscholar.org/CorpusID:1399943 [Accessed 20.10.2023]

10. Cao Y., Li S., Wijmans E. (Cross-) Browser Fingerprinting via OS and Hardware Level Features. *NDSS' 2017, San Diego, USA, 26 February – 1 March 2017*. 2017. DOI:10.14722/ndss.2017.23152

11. Englehardt S., Narayanan A. Online tracking: A 1-million-site Measurement and Analysis. *Proceedings of the Conference on Computer and Communications Security, 2016 ACM SIGSAC, 24–28 October 2016, Vienna, Austria*. New York: Association for Computing Machinery; 2016. p.1388–1401. DOI:10.1145/2976749.2978313

12. Sjösten A., Van Acker S., Sabelfeld A. Discovering Browser Extensions via Web Accessible Resources. *Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy, CODASPY '17, 22–24 March 2017, Scottsdale, USA*. New York: Association for Computing Machinery; 2017. p.329–336. DOI:10.1145/3029806.3029820

13. Sanchez-Rola I., Santos I., Balzarotti D. Extension Breakdown: Security Analysis of Browsers Extension Resources Control Policies. *Proceedings of the 26th USENIX Conference on Security Symposium, USENIX Security 17, 16–18 August 2017, Vancouver, Canada*. Berkeley: USENIX Association; 2017. p.679–694.

14. Starov O., Nikiforakis N. Xhound: Quantifying the Fingerprintability of Browser Extensions. *Proceedings of the Symposium on Security and Privacy, SP, 22–26 May 2017, San Jose, USA)*. IEEE; 2017. p.941–956. DOI:10.1109/SP.2017.18

15. Mowery K., Bogenreif D., Yilek S., Shacham H. *Fingerprinting Information in JavaScript Implementations*. 2012. URL: https://search.iczhiku.com/paper/hgdOSDNQ7g2K8zv8.pdf [Accessed 20.10.2023]

16. Nakibly G., Shelef G., Yudilevich S. Hardware Fingerprinting Using HTML5. *arXiv:1503.01408*. 2015. DOI:10.48550/arXiv.1503.01408

17. Olejnik Ł., Acar G., Castelluccia C., Diaz C. The leaking battery. *Proceedings of the International Workshop on Data Privacy Management International Workshop on Quantitative Aspects in Security Assurance*. 2015. p.254–263. DOI:10.1007/978-3-319-29883-2_18

18. Vastel A., Laperdrix P., Rudametkin W., Rouvoy R. FP-STALKER: Tracking Browser Fingerprint Evolutions. *Proceedings of the Symposium on Security and Privacy, SP, USA, 20–24 May 2018, San Francisco*. IEEE; 2018. p.728–741. DOI:10.1109/SP.2018.00008

19. Laperdrix P., Rudametkin W., Baudry B. Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints. *Proceedings of the Symposium on Security and Privacy, SP, 22–26 May 2016, San Jose, USA.* IEEE; 2016. p.878–894. DOI:10.1109/SP.2016.57

20. Gómez-Boix A., Laperdrix P., Baudry B. Hiding in the Crowd: an Analysis of the Effectiveness of Browser Fingerprinting at Large Scale. *Proceedings of the World Wide Web Conference, 23–27 April 2018, Lyon, France.* 2018. p.309–318. DOI:10.1145/3178876.3186097

21. *Operation Fingerprint*. A look into several Angler Exploit Kit malvertising campaigns. 2016. URL: https://malwarebytes.app.box.com/v/operation-fingerprint [Accessed 26.04.2023]

22. *LexisNexis Risk Solutions*. ThreatMetrix – Cybersecurity Risk Management. URL: https://risk.lexisnexis.com/products/threatmetrix [Accessed 26.04.2023]

23. *Imperva*. The Evolution of Hi-Def Fingerprinting in Bot Mitigation. 2018. URL: https://www.imperva.com/blog/the-evolution-of-hi-def-fingerprinting-in-bot-mitigation [Accessed 26.04.2023]

24. *MaxMind*. Track Devices. 2023. URL: https://dev.maxmind.com/minfraud/track-devices [Accessed 26.04.2023]

25. *HUMAN Bot Defender*. Safeguard Websites, Mobile Apps & APIs From Bots. 202]. URL: https://www.humansecurity.com/products/human-bot-defender#scroll-down [Accessed 26.04.2023]

26. *IPQualityScore*. Device Fingerprinting. 2023. URL: https://www.ipqualityscore.com/device-fingerprinting [Accessed 26.04.2023]

27. *Radware*. Comprehensive Bot Management. 2023. URL: https://www.radware.com/products/bot-manager [Accessed 26.04.2023]

28. *Sift*. Fraud Detection Software for Secure Growth. 2023. URL: https://sift.com/products/digital-trust-safety-platform [Accessed 26.04.2023]

29. *SecurAuth*. Device Recognition. 2023. URL: https://docs.secureauth.com/2104/en/device-recognition.html [Accessed 26.04.2023]

30. *TransUnion*. TruValidate. 2023. URL: https://www.transunion.com/solution/truvalidate [Accessed 26.04.2023]

31. Murashko Yu.V., Papaev B.N. Increasing the Accuracy of User Identification by Digital Fingerprint Using a Two-Stage Approach. *X International Scientific and Practical Conference on Prospective scientific research: experience, problems and prospects of development*. 2023. p.191-195.

32. Murashko Yu.V. User Identification in Network Traffic. Proceedings of the All-Russian Scientific and Technical Conference on Actual Problems of Radio Electronics and Telecommunications, 25–28 April 2023, Samara, Russian Federation. 2023. p.166-169.

33. Sultana M., Paul P.P., Gavrilova M. A Concept of Social Behavioral Biometrics: Motivation, Current Developments, and Future Trends. *Proceedings of the International Conference on Cyberworlds, 06–08 October 2014, Santander, Spain*. IEEE; 2014. p.271–278. DOI:10.1109/CW.2014.44

34. Murashko Yu.V. Identification of network users by their behavior. Proceedings of the IX All-Russian Scientific and Technical Conference on Fundamental and Applied Aspects of Computer Technologies and Information Security, 10–15 April 2023, Taganrog, Russian Federation). Rostov-on-Donu: Southern Federal University Publ.; 2023. p.54–56.

35. Rybnik M., Tabedzki M., Adamski M., Saeed K. An Exploration of Keystroke Dynamics Authentication Using Non-fixed Text of Various Length. *Proceedings of the International Conference on Biometrics and Kansei Engineering, 05–07 July 2013, Tokyo, Japan*. IEEE; 2013. p.245–250. DOI:10.1109/ICBAKE.2013.48

36. Shimshon T., Moskovitch R., Rokach L., Elovici Y. Continuous Verification Using Keystroke Dynamics. *Proceedings of the International Conference on Computational Intelligence and Security, 11–14 December 2010, Nanning, China*. IEEE; 2010. p.411–415. DOI:10.1109/CIS.2010.95

37. Teh P.S., Teoh A.B.J., Yue S. A Survey of Keystroke Dynamics Biometrics. *The Scientific World Journal*. 2013;2013:408280. DOI:10.1155/2013/408280

38. Tsimperidis I., Yoo P.D., Taha K., Mylonas A., Katos V. R²BN: An adaptive Model for Keystroke-Dynamics-Based Educational Level Classification. *IEEE Transactions on Cybernetics*. 2018;50(2):525–535. DOI:10.1109/TCYB.2018.2869658

39. Alshanketi F., Traore I., Ahmed A.A. Improving Performance and Usability in Mobile Keystroke Dynamic Biometric Authentication. *Proceedings of the IEEE Security and Privacy Workshops, SPW, 22–26 May 2016, San Jose, USA*. IEEE; 2016. p. 66–73. DOI:10.1109/SPW.2016.12

40. Ali M.L., Thakur K., Tappert C.C., Qiu M. Keystroke Biometric User Verification Using Hidden Markov Model. *Proceedings of the 3rd International Conference on Cyber Security and Cloud Computing, CSCloud, 25–27 June 2016, Beijing, China*. IEEE; 2016. p.204–209. DOI:10.1109/CSCloud.2016.23

41. Krishnamoorthy S., Rueda L., Saad S., Elmiligi H. Identification of User Behavioral Biometrics for Authentication Using Keystroke Dynamics and Machine Learning. *Proceedings of the 2nd International Conference on Biometric Engineering and Applications, ICBEA '18, 16–18 May 2018, Amsterdam, Netherlands*. New York: Association for Computing Machinery; 2018. p.50–57. DOI:10.1145/3230820.3230829

42. Higashino J. Signature Verification System on Neuro-Computer. *Proceedings of the 11th International Conference on Pattern Recognition, IAPR, 30 August – 3 September 1992, Hague, Netherlands,* vol.3. 1992. p.517–521.

43. Everitt R.A.J., McOwan P.W. Java-based internet biometric authentication system. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2003;25(9):1166–1172. DOI:10.1109/TPAMI.2003.1227991

44. Ahmed A.A.E., Traore I. A New Biometric Technology Based on Mouse Dynamics. *IEEE Transactions on Dependable and Secure Computing*. 2007;4(3):165–179. DOI:10.1109/TDSC.2007.70207

45. Antal M., Szabó L.Z. Biometric Authentication Based on Touchscreen Swipe Patterns. *Procedia Technology*. 2016;22: 862–869. DOI:10.1016/j.protcy.2016.01.061

46. Khan H., Hengartner U. Towards application-centric implicit authentication on smartphones. *Proceedings of the 15th Workshop on Mobile Computing Systems and Applications, 26–27 February 2014, Santa Barbara, USA*. New York: Association for Computing Machinery; 2014. P. 10. p.1–6. DOI:10.1145/2565585.2565590

47. Ferrero R., Gandino F., Montrucchio B., Rebaudengo M., Velasco A., Benkhelifa I. On gait recognition with smartphone accelerometer. *Proceedings of the 4th Mediterranean Conference on Embedded Computing, MECO, 14–18 June 2015, Budva, Montenegro*. IEEE; 2015. p.368–373. DOI:10.1109/MECO.2015.7181946

48. Fantana A.L., Ramachandran S., Schunck C.H., Talamo M. Movement based biometric authentication with smartphones. *Proceedings of the International Carnahan Conference on Security Technology, ICCST, 21–24 September 2015, Taipei, Taiwan*. IEEE; 2015. p.235–239. DOI:10.1109/CCST.2015.7389688

49. Laghari A., Waheed-ur-Rehman, Memon Z.A. Biometric authentication technique using smartphone sensor. *Proceedings of the 13th International Bhurban Conference on Applied Sciences and Technology, IBCAST, 12–16 January 2016, Islamabad, Pakistan*. IEEE; 2016. p.381–384. DOI:10.1109/IBCAST.2016.7429906

50. Hong F., Wei M., You S., Feng Y., Guo Z. Waving authentication: your smartphone authenticate you on motion gesture. *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems, 18–23 April 2015, Seoul, Republic of Korea*. New York: Association for Computing Machinery; 2015. p.263–266. DOI:10.1145/2702613.2725444

51. Ehatisham-ul-Haq M., Azam,M.A., Naeem U., Amin Y., Loo J. Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing. *Journal of Network and Computer Applications*. 2018;109:24–35. DOI:10.1016/j.jnca.2018.02.020

52. Feng T., Zhao X., Shi W. Investigating Mobile Device Picking-up motion as a novel biometric modality. *Proceedings of the Sixth International Conference on Biometrics on Theory, Applications and Systems, BTAS, 29 September – 02 October 2013, Arlington, USA.* IEEE; 2013. DOI:10.1109/BTAS.2013.6712701

53. Oak R., Khare M. A Novel Architecture for Continuous Authentication Using Behavioural Biometrics. *Proceedings of the International Conference on Current Trends in Computer, Electrical, Electronics and Communication, India, 8–9 September 2017, CTCEEC, Mysore.* 2017. p.767–771. DOI:10.1109/CTCEEC.2017.8455040

54. Reynolds D.A. An Overview of Automatic Speaker Recognition Technology. *Proceedings of the International Conference on Acoustics, Speech, and Signal Processing, ICASSP, 13–17 May 2002, Orlando, USA, vol.4*. IEEE; 2002. p.4072–4075.

55. Ravanelli M., Bengio Y. Speaker Recognition from Raw Waveform with SincNet. *Proceedings of the Spoken Language Technology Workshop, SLT, 18–21 December 2018, Athens, Greece*. IEEE; 2018. p.1021–1028. DOI:10.1109/SLT.2018.8639585

56. Arik S., Chen J., Peng K., Ping W., Zhou Y. Neural Voice Cloning with a Few Samples. *Proceedings of the 32nd Conference on Neural Information Processing Systems, NeurIPS 2018, 3–8 December 2018, Montréal, Canada*, vol.31. 2018.

57. Hu Q., Marchi E., Winarsky D., Stylianou Y., Naik D., Kajarekar S. Neural Text-to-Speech Adaptation from Low Quality Public Recordings. *Proceedings of the 10th ISCA Workshop on Speech Synthesis, SSW 10, 20-22 September 2019, Vienna, Austria, vol.10*. 2019. p.24–28. DOI:10.21437/SSW.2019-5

58. Kameoka H. Stargan-vc: Non-parallel many-to-many voice conversion using star generative adversarial networks. *Proceedings of the Spoken Language Technology Workshop, SLT, 18–21 December 2018, Athens, Greece*. IEEE; 2018. p.266–273. DOI:10.1109/SLT.2018.8639535

59. Rebryk Y., Beliaev S. Convoice: Real-Time Zero-Shot Voice Style Transfer with Convolutional Network. *arXiv:2005.07815*. 2020. DOI:10.48550/arXiv.2005.07815

60. Wu D.Y., Chen Y.H., Lee H.Y. Vqvc+: One-Shot Voice Conversion by Vector Quantization and U-Net Architecture. *arXiv:2006.04154*. 2020. DOI:10.48550/arXiv.2006.04154

61. Wenger E., Bronckers M., Cianfarani C., Cryan J., Sha A., Zheng H., et al. "Hello, It's Me": Deep Learning-based Speech Synthesis Attacks in the Real World. *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, 15–19 November 2021, Virtual Event Republic of Korea*. New York: Association for Computing Machinery; 2021. p.235–251. DOI:10.1145/3460120.3484742

62. Janicki A., Alegre F., Evans N. An assessment of automatic speaker verification vulnerabilities to replay spoofing attacks. *Security and Communication Networks*. 2016;9(15):3030–3044. DOI:10.1002/sec.1499

63. Kinnunen T., Sahidullah M., Delgado H., Todisco M., Evans N. Yamagishi J., et al. *The ASVspoof 2017 Challenge: Assessing the Limits of Replay Spoofing Attack Detection*. 2017. URL: https://www.eurecom.fr/~evans/papers/pdfs/5235.pdf [Accessed 22.10.2023]

64. Gao Y., Lian J., Raj B., Singh R. Detection and Evaluation of Human and Machine Generated Speech in Spoofing Attacks on Automatic Speaker Verification Systems. *Proceedings of the Spoken Language Technology Workshop, SLT, 19–22 January 2021, Shenzhen, China*. IEEE; 2021. p.544–551. DOI:10.1109/SLT48900.2021.9383558

65. Vestman V., Kinnunen T., Hautamäki R.G., Sahidullah Md. Voice Mimicry Attacks Assisted by Automatic Speaker Verification. *Computer Speech & Language*. 2020;59:36–54. DOI:10.1016/j.csl.2019.05.005

66. Masuko T., Hitotsumatsu T., Tokuda K., Kobayashi T. On the security of HMM-based speaker verification systems against imposture using synthetic speech*. Proceedings of the Sixth European Conference on Speech Communication and Technology, EUROSPEECH 1999, 5-9 September 1999, Budapest, Hungary*. 1999.

67. Mukhopadhyay D., Shirvanian M., Saxena N. All Your Voices are Belong to Us: Stealing Voices to Fool Humans and Machines. *Proceedings of the 20th European Symposium on Research in Computer Security, ESORICS 2015, 21–25 September 2015, Vienna, Austria. Lecture Notes in Computer Science,* vol.9327. Cham: Springer; 2015. p.599–621. DOI:10.1007/978-3-319-24177-7_30

68. Partila P., Tovarek J., Ilk G.H., Rozhon J., Voznak M. Deep Learning Serves Voice Cloning: How Vulnerable Are Automatic Speaker Verification Systems to Spoofing Trials? *IEEE Communications Magazine*. 2020;58(2):100–105. DOI:10.1109/MCOM.001.1900396

69. Ahmed M.E., Kwak I.Y., Huh J.H., Kim I., Oh T., Kim H. Void: A fast and light voice liveness detection system. *Proceedings of the 29th USENIX Security Symposium, USENIX Security, 12–14 August 2020.* 2020. p.2685–2702.

70. AlBadawy E.A., Lyu S., Farid H. Detecting AI-Synthesized Speech Using Bispectral Analysis. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*. 2019. p.104–109.

71. Huang C., Lin Y.Y., Lee H., Lee L. et al. Defending Your Voice: Adversarial Attack on Voice Conversion. *Proceedings of the Spoken Language Technology Workshop, SLT, 19–22 January 2021, Shenzhen, China*. IEEE; 2021. p.552–559. DOI:10.1109/SLT48900.2021.9383529

72. Kobayashi R., Yamaguchi R.S. A Behavior Authentication Method Using Wi-Fi BSSIDs around Smartphone Carried by a User. *Proceedings of the Third International Symposium on Computing and Networking, CANDAR, 08–11 December 2015, Sapporo, Japan*. IEEE; 2015. p.463–469. DOI:10.1109/CANDAR.2015.45

73. Bassu D., Cochinwala M., Jain A. A new mobile biometric based upon usage context. *Proceedings of the International Conference on Technologies for Homeland Security, HST, 12–14 November 2013, Waltham, USA*. IEEE; 2013. p.441–446. DOI:10.1109/THS.2013.6699045

74. Branscomb A.S. *Behaviorally Identifying Smartphone Users*. Master's Thesis. Raleigh: North Carolina State University; 2013.

75. Neal T.J., Woodard D.L., Striegel A.D. Mobile device application, Bluetooth, and Wi-Fi usage data as behavioral biometric traits. *Proceedings of the 7th International Conference on Biometrics Theory, Applications and Systems, BTAS, 08–11 September 2015, Arlington, USA*. IEEE; 2015. p.1–6. DOI:10.1109/BTAS.2015.7358777

76. Fridman L., Weber S., Greenstadt R., Kam M. Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location. *IEEE Systems Journal*. 2016;11(2):513–521. DOI:10.1109/JSYST.2015.2472579

77. Brocardo M.L., Traore I., Saad S., Woungang I. Authorship verification for short messages using stylometry. *Proceedings of the International Conference on Computer, Information and Telecommunication Systems, CITS, 07–08 May 2013, Athens, Greece*. IEEE; 2013. p.1–6. DOI:10.1109/CITS.2013.6705711

78. Cao H., Bao T., Yang Q., Chen E. An effective approach for mining mobile user habits. *Proceedings of the 19th ACM International Conference on Information and Knowledge Management, CIKM 2010, 26–30 October 2010, Toronto, Canada*. New York: Association for Computing Machinery; 2010. p.1677–1680. DOI:10.1145/1871437.1871702
79. Jang J., Yun J., Woo J., Kim H.K. Andro-profiler: anti-malware system based on behavior profiling of mobile malware. *Proceedings of the 23rd International Conference on World Wide Web, WWW '14 Companion, 7–11 April 2014, Seoul, Korea*. New York: Association for Computing Machinery, 2014. p.737–738. DOI:10.1145/2567948.2579366
80. *Github*. UMDAA-02 Dataset. 2018. URL: https://umdaa02.github.io [Accessed 26.04.2023]
81. *Github*. BiDAlab/HuMIdb. 2020. URL: https://github.com/BiDAlab/HuMIdb [Accessed 26.04.2023]
82. *Github*. BiDAlab/MobileB2C_BehavePassDB. 2022. URL: https://github.com/BiDAlab/MobileB2C_BehavePassDB [Accessed 26.04.2023]
83. Mahbub U., Sarkar S., Patel V.M., Chellappa R. Active user authentication for smartphones: A challenge data set and benchmark results. *Proceedings of the 8th international conference on biometrics theory, applications and systems, BTAS, 06–09 September 2016, Niagara Falls, USA*. IEEE; 2016. p.1–8. DOI:10.1109/BTAS.2016.7791155
84. Acien A., Morales A., Fierrez J., Vera-Rodriguez R., Delgado-Mohatar O. BeCAPTCHA: Behavioral bot detection using touchscreen and mobile sensors benchmarked on HuMIdb. *Engineering Applications of Artificial Intelligence*. 2021;98:104058. DOI:10.1016/j.engappai.2020.104058
85. Stragapede G., Vera-Rodriguez R., Tolosana R., Morales A. BehavePassDB: Public Database for Mobile Behavioral Biometrics and Benchmark Evaluation. *Pattern Recognition*. 2023;134:109089. DOI:10.1016/j.patcog.2022.109089
86. Ananya, Singh S. Keystroke Dynamics for Continuous Authentication. *Proceedings of the 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 11–12 January 2018, Noida*. IEEE; 2018. p.205–208. DOI:10.1109/CONFLUENCE.2018.8442703
87. Mondal S., Bours P. Continuous authentication using mouse dynamics. *Proceedings of the International Conference of the BIOSIG Special Interest Group, BIOSIG, 05–06 September 2013, Darmstadt, Germany*. IEEE; 2013. p.1–12.
88. *Plurilock*. Plurilock AI – Least privilege CASB, DLP with DEFEND technology. 2016. URL: https://plurilock.com [Accessed 26.04.2023]
89. *ThreatMark*. ThreatMark Fraud Prevention Solution. 2015. URL: https://www.threatmark.com [Accessed 26.04.2023]
90. *Aculab*. VoiSentry. 2018. URL: https://www.aculab.com/biometric-technologies/voisentry [Accessed 26.04.2023]
91. *Cynet*. User Behavior Analytics (UBA). 2018. URL: https://www.cynet.com/platform/user-behaviour-analytics [Accessed 26.04.2023]
92. *UnifyID*. Authentication platform. 2015. URL: https://unify.id [Accessed 26.04.2023]
93. *Craft.co*. SecuredTouch Company Profile – Office Locations, Competitors, Financials, Employees, Key People, News. 2016. URL: https://craft.co/securedtouch [Accessed 26.04.2023]

Статья поступила в редакцию 05.07.2023; одобрена после рецензирования 28.08.2023; принята к публикации 17.10.2023.
The article was submitted 05.07.2023; approved after reviewing 28.08.2023; accepted for publication 17.10.2023.

Информация об авторах:

ОСИН Андрей Владимирович
кандидат технических наук, доцент кафедры «Информационная безопасность» Московского технического университета связи и информатики
https://orcid.org/0000-0002-6384-9365

МУРАШКО Юрий Викторович
аспирант кафедры «Информационная безопасность» Московского технического университета связи и информатики
https://orcid.org/0009-0003-6448-8412