Вопросы безопасности
*Правильная ссылка на статью:*
Цветкова А.Д. — Сведения о компьютерном почерке: проблемы поиска баланса между свободой личности и безопасностью государства // Вопросы безопасности. – 2023. – № 3. DOI: 10.25136/2409-7543.2023.3.43749 EDN: ZSSKED URL: https://nbpublish.com/library_read_article.php?id=43749

# Сведения о компьютерном почерке: проблемы поиска баланса между свободой личности и безопасностью государства

**Цветкова Анна Денисовна**

ORCID: 0000-0002-1631-9265

Студент, Институт юстиции, Уральский государственный юридический университет имени В. Ф. Яковлева"

620034, Россия, Свердловская область, г. Екатеринбург, ул. Колмогорова, 54

at@crimlib.info

Статья из рубрики "Человек и гражданин в системе безопасности"

**DOI:**

10.25136/2409-7543.2023.3.43749

**EDN:**

ZSSKED

**Дата направления статьи в редакцию:**

09-08-2023

**Аннотация:** Настоящее исследование посвящено вопросам внедрения систем биометрической идентификации в правоохранительную деятельность. Особое внимание автор уделяет феномену компьютерного почерка, подробно рассматривая конституционно-правовые аспекты использования знаний о нём. Для этого задействуется широкий методологический аппарат: сравнительно-правовой метод, метод аналогии, дедукция, метод моделирования и др. Проводится сопоставление Российской практики и потенциала дальнейшего развития с опытом зарубежных государств как в регулировании общих вопросов биометрических персональных данных, так и в ситуациях легальной регламентации именно сведений о компьютерном почерке. Автор исследует, каким образом одновременно решить задачи раскрытия и расследования преступлений, в которых доказательственными материалами выступают напечатанные тексты, и при этом сохранить права человека на неприкосновенность личной жизни, личную и семейную тайну, анонимность в Интернете. Отмечается, что компьютерный почерк является достаточно молодым феноменом для юридической науки; до сих пор отсутствует глубокое его исследование с позиций данной области знаний. Настоящая

работа представляет собой лишь начало в постижении рассматриваемой тематики. В ней ставятся базовые вопросы: допустимо ли использовать знания о компьютерном почерке, как их следует защищать и где хранить, нужно ли ограничивать существующий коммерческий интерес в их использовании. В итоге автор приходит к следующим выводам: сведения о компьютерном почерке допустимо и необходимо собирать, так как это позволит уменьшить посягательства на естественные права человека и гражданина. Для такого сбора необходимо использовать централизованную государственную систему, в которой реализуются все требования к безопасности критической информационной инфраструктуры. Однако до введения такой системы в эксплуатацию необходимо поддерживать коммерческие компании в соответствующих разработках и обязать их предоставлять сведения о компьютерном почерке пользователей по запросам уполномоченных лиц.

**Ключевые слова:**

компьютерный почерк, клавиатурный почерк, биометрические персональные данные, биометрия, динамическая биометрическая характеристика, компьютерные преступления, идентификация исполнителя, напечатанный текст, конституционные права, личная тайна

*Исследование выполнено за счет гранта Российского научного фонда № 23-78-10011, https://rscf.ru/project/23-78-10011/*

В последние годы всё более стремительными темпами информационные технологии проникают в нашу жизнь. В России и за рубежом стали говорить о так называемых информационных правах граждан: праве на забвение, праве определять свою «цифровую личность», праве на доступ к сети Интернет и т. д. [1, с. 8–31]. Однако любое технологическое развитие актуализирует проблему достижения баланса между свободой и безопасностью: так, с одной стороны, многие люди видят в компьютерных системах средство полной анонимизации, создания вымышленной личности цифрового профиля с теми характеристиками, которые сам человек желает закрепить [2, с. 142]. Одновременно с этим, с каждым годом растёт число компьютерных преступлений, особенно если подходить к их пониманию в широком, криминалистическом смысле [3, с. 167]. Данный факт отмечается не только научным сообществом: так, на Экономическом и гуманитарном форуме Россия-Африка, прошедшем 27–28 июля 2023 года в Санкт-Петербурге указывалось, что отечественные информационные системы чаще, нежели это происходит в других странах, подвергаются кибератакам. Соответственно, государство заинтересовано в максимальном контроле виртуальной среды. В частности, сохраняя право пользователей на анонимность, оно желает выработать механизм идентификации граждан, деанонимизации их личности в случае возникновения такой необходимости.

Указанную задачу весьма успешно разрешают биометрические технологии, которые позволяют помимо этого повысить уровень личной информационной безопасности посредством настройки систем двухфакторной аутентификации для доступа в систему [4, с. 49]. Именно их исследование с позиций перспектив внедрения в общественную жизнь и является предметом настоящего исследования.

Биометрические технологии представляют собой инструментальные решения обработки биометрических персональных данных человека [5, с. 242]. В науке последние принято делить на статические и динамические (поведенческие) [6, с. 2; 7, с. 35; 8, с. 83]. Однако

представляется, что данный подход нельзя признать в полной мере допустимым для использования в российских юридических исследованиях. Это связано с тем, что статья 11 Федерального закона от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023) «О персональных данных» делит все персональные данные на биологические физиологические. Таким образом, далее нами будут использоваться легально установленные категории с той оговоркой, что содержание физиологических биометрических данных совпадает с динамическими и поведенческими, раскрывающимися в большинстве научных исследований по соответствующей теме.

Среди всех биометрических технологий в России наиболее распространёнными являются те, которые позволяют идентифицировать человека по папиллярному узору пальцев рук, изображению лица и радужной оболочке [9]. Однако биометрия включает в себя намного более обширный перечень идентификационно-значимых признаков [10; 11, с. 14], а современный уровень технологического развития позволяет говорить о существовании обширного потенциала для разработки соответствующих биометрических технологий. В части компьютерных преступлений наиболее приоритетным представляется обработка сведений о компьютерном почерке лица, так как всеми исследователями этого феномена отмечается его сравнительная дешевизна и простота, поскольку фиксация не требует дорогостоящего оборудования [12, с. 64].

Поясним, что компьютерный почерк представляет собой физиологическую биометрическую характеристику личности, объединяющую в себе совокупность навыков и привычек взаимодействия пользователя с устройствами-манипуляторами при создании текста. Наибольшую информативность в его структуре представляют сведения о специфике клавиатурного набора: сила нажатия [13], динамика ввода [14, с. 240], скорость печати [15, с. 17], длительность интервала между нажатиями [16, с. 583] и др.

Целью настоящего исследования является доказать перспективность и допустимость с точки зрения соблюдения конституционных норм широкого распространения технологии идентификации и аутентификации пользователей компьютерных устройств на основе информации об их компьютерном (клавиатурном) почерке. Для этого нами были задействованы как общенаучные, так и специальные методы. Наиболее значимыми из всех явились: метод аналогии (при проецирование правовых режимов уже реализуемых биометрических систем на новые технологии), дедукция (при проецировании генеральных признаков биометрических данных на отдельные частные примеры), сравнительно-правовой (при сопоставлении законодательного регулирования биометрических данных в разных странах), системный (для согласования доктринальных и легальных подходов), метод моделирования (при конструировании возможных сценариев расширения числа применяемых в целях повышения государственной безопасности биометрических технологий) и др.

Компьютерный почерк может рассматривается в качестве персональных данных [15, с. 17], которые, согласно п. 1 ч. 1 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», определяются как «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)». Более того, рассматриваемый феномен, о чём в первую очередь говорят все его исследователи, входит в категорию биометрических персональных данных [4, с. 49; 17, с. 583; 18, с. 128], которые, как отмечается в научной литературе с опорой на ст. 11 указанного закона, обладают двумя чертами: «во-первых, характеризуют физиологические и биологические особенности человека, на основании

которых можно установить его личность, и, во-вторых, используются оператором персональных данных для установления личности субъекта» [19, с. 116]. При этом подчёркивается, что биометрическими персональными данными могут выступать те сведения, которые непосредственно используются для идентификации, а не только теоретически пригодны для неё [19, с. 116]. Сведения о компьютерном почерке характеризуют физиологическую особенность человека и позволяют определить конкретного носителя, а также используются сегодня на частном уровне для идентификации пользователя компьютерного устройства [20–22]. Можно сделать вывод (и это подтверждается всеми исследователями [10, с. D-116; 23, с. 157; 24, с. 171]), что компьютерный почерк является функциональной биометрической характеристикой личности.

В связи с этим существование феномена компьютерного почерка создаёт для науки конституционного права значительное пространство для исследования, порождая следующие вопросы:

1) допустимо ли с точки зрения конституционных прав граждан собирать сведения об их компьютерном почерке;

2) каким образом должна производиться защита данных о компьютерном почерке лица [25, с. 165];

3) где должны сохраняться сведения о компьютерном почерке;

4) следует ли ограничивать коммерческие организации, которые «также заинтересованы в сборе и обработке персональных данных с целью создания новых бизнес-моделей, персонализации предоставляемых товаров и услуг, максимально эффективного использования инновационных технологий в конкурентной борьбе, защите собственных интересов при разрешении споров» [26, с. 74] (в частности, сведения о компьютерном почерке пользователей берутся за основу для разработки более удобных, эргономичных клавиатур, что создаёт конкурентное преимущество на рынке комплектующих компьютерных устройств), и как возможно осуществить это ограничение, и др.

Однако несмотря на достаточно длительную историю исследований, посвящённых рассматриваемому нами феномену, начавшуюся в 1970-х годах [10, с. D-116–D-122], подавляющее большинство работ до сих пор не выходит за рамки компьютерно-технической области знаний. Правовые же исследования, если и имеются, то игнорируют, за редким исключением, аспекты легального внедрения систем фиксации показателей компьютерного почерка (в качестве исключения можно назвать работы И. З. Фёдорова [27], тогда как, например, Е. И. Фойгель, также затрагивающая тему компьютерного почерка не анализируют вопрос получения сведений о нём с правовой точки зрения [28, с. 105]).

Решение обозначенных выше вопросов – предметная область государственно- и публично-правовых наук – и работа в указанном направлении необходима для создания юридически обоснованной возможности расширения сфер применения биометрических технологий. В настоящей же работе мы постараемся заложить основу для дальнейших исследований в указанном направлении, кратко ответив на поставленные проблемные вопросы. При этом отметим, что они представляют собой лишь начальное звено, но не исчерпывают всей глубины данной темы.

1. Первый вопрос представляется наиболее сложным, поскольку располагается не

столько в рамках науки, сколько в сфере философии, заявляя вечную дилемму: свобода или безопасность. В начале настоящей статьи мы уже указывали на данное противоречие при рассмотрении вопросов использования биометрических технологий, сейчас же подчеркнём следующее. По нашему мнению, конституционные права человека в большей степени будут соблюдаться, если государство начнёт централизовано собирать информацию о компьютерном почерке лиц, действующих в виртуальном пространстве. Можно провести аналогию с паспортным контролем в аэропортах: сотрудники службы безопасности видят всё, что пассажир собирается пронести с собой в зону вылета, но это позволяет предотвратить теракты, сохранив жизни мирным гражданам. Так же и со сведениями о компьютерном почерке: в информационную систему будут поступать сведения об индивидуализирующих исполнителя характеристиках набираемого на компьютерном устройстве текста, однако это позволит вовремя выявить экстремистов, педофилов и иных злоумышленников, распространяющих через Интернет противоправную информацию [29, с. 575–576]. К тому же необходимо учитывать, что такие объёмы информации явно не будут обрабатываться человеком, так как его ресурсов для этого недостаточно [30, с. 5; 31, с. 23]. Все основные операции по сбору, накоплению, хранению, распределению будут осуществляться автоматизировано, тогда как человек – уполномоченный представитель государства – сможет получить доступ к этим сведениям только в ситуации необходимости, при которой допускается обработка персональных данных субъекта без его согласия (п. 2–11 ч. 1 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных») .

2. Потребность в защите информации о компьютерном почерке лица связана не только с его отнесением к персональным данным, которые должны охраняться в принципе, но и с повышенным риском для неприкосновенности личной жизни и тайны, вызванным спецификой технологии получения сведений о компьютерном почерке. Специальные программы, программно-аппаратные устройства или встроенные модули операционной системы (далее, совокупно системы, захватывающие показатели компьютерного почерка, мы будем, допуская определённую долю условности, именовать кейлоггерами) фиксируют и сохраняют информацию о каждой нажатой клавише с указанием временных меток [32, с. 48]. Таким образом, сведения о компьютерном почерке оказываются непосредственно связанными с конкретным набираемым текстом. Помимо этого, отдельные кейлоггеры также отслеживают посещённые сайты, запущенные программы [33]. Постоянный централизованный сбор, о котором подробнее будет сказано далее, с одной стороны, повышает риск утечки этих сведений из-за противоправных действий злоумышленников, а с другой стороны, делает эту информацию полностью доступной для государства. В связи с этим, некоторыми авторами предлагается кодировать сведения о компьютерном почерке так, чтобы система теряла связь с набранным текстом и посредством искусственной интеллектуальной обработки предлагала человеку только обезличенную выдачу с информацией о тождественности лица, набиравшего сравниваемые тексты, не демонстрируя те вводные, на основе которых было принято решение [34, с. 55]. Однако представляется, что использование таких технологических решений приемлемо только для «домашнего» использования компьютерного почерка при внедрении в системы контроля допуска. То есть при таком обезличивании невозможно обращаться к данным о компьютерном почерке для решения, например, задач раскрытия и расследования преступлений, где необходимо идентифицировать лицо, напечатавшее тот или иной текст. Поэтому перспективным, на наш взгляд, будет решать проблему задействованием правовых, а не технологических механизмов. Однако это не исключает необходимости соблюдения всех правил безопасности, предъявляемых к защите

критической информационной инфраструктуры Российской Федерации [35, с. 16].

3. Одним из правовых механизмов, на которые мы указали в предыдущем пункте, может выступать детальное регулирование вопросов фиксации и использования сведений о компьютерном почерке. Для начала можно добавить упоминание о нём в ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», раскрыв наряду с остальными основными понятиями. Расширение сфер его применения может потребовать внесения соответствующих дополнений и в иные нормативно-правовые акты, существующего сегодня указания на существование компьютерного почерка исключительно в ГОСТах в скором времени будет недостаточно[36, с. 123]. При этом считаем целесообразным в некоторых вопросах обратиться к опыту других государств, где, в частности существует отдельное регулирование отношений, связанных с оборотом биометрических персональных данных, а также на законодательном уровне закреплён этот статус за компьютерным почерком (см. например, отдельные штаты США, в частности Калифорнию, Китай, Европейский Союз и др.) [32; 19, с. 97–116].

Помимо этого, можно на законодательном уровне установить обязанность для всех разработчиков программного обеспечения внедрять в свои компьютерные устройства кейлоггеры и предоставлять сведения о компьютерном почерке пользователей по запросу представителей государства. Однако более приоритетным видится сценарий, при котором будет существовать обязанность всех устанавливать лицензионный государственный кейлоггер, настроенный на передачу информации в режиме реального времени в государственную базу данных. Последняя может представлять из себя как полностью автономную систему, так и выделенный блок в Единой биометрической системе. Считаем, что это позволило бы облегчить решение задач идентификации исполнителя напечатанного текста в рамках деятельности по раскрытию и расследованию преступлений. Вместе с тем, повышенные требования к защищённости государственных баз данных с большей вероятностью гарантируют сохранность информации о компьютерном почерке лиц именно в централизованной федеральной системе.

Оговоримся, что мы не считаем правильным рассматривать в контексте правового регулирования вопросы использования компьютерного почерка в целях обеспечения персональной информационной безопасности – наиболее развитой сферы его использования, о чём свидетельствуют научные исследования и практические разработки [37, с. 191], поскольку, на наш взгляд, абсолютная юридизация общественных отношений может привести к стагнации развития, и не требуется в тех сферах, которые в норме функционируют без правовых рамок. Однако это не означает, что те аспекты применения компьютерного почерка, которые представляют наибольший интерес для специалистов в области компьютерных технологий, не могут быть заимствованы правовой сферой. Так, например, детализация общих вопросов обращения к компьютерному почерку для обеспечения информационной безопасности позволяет говорить об адаптивности описанных моделей контроля доступа к определённым системам, отдельной информации в различных специальных сферах деятельности. Например, констатируется актуальная необходимость разработки новых систем управления доступом к автоматизированным системам органов внутренних дел Российской Федерации, главным образом, с целью обеспечения защищённости критической информационной инфраструктуры государства [38, с. 22], что, однако, должно рассматриваться в рамках информационного права.

4. Что же касается коммерческих лиц, то на настоящем этапе не следует вводить какие-

либо запретительные меры, однако следует предусмотреть обязанность для компаний, отбирающих сведения о компьютерном почерке, обязанность предупреждать пользователей об этом и получать их согласие, например по модели, введённой для Cookie-файлов [39]. Представляется даже, напротив, весьма полезным тот факт, что коммерческие компании сегодня фиксируют сведения о компьютерном почерке, поскольку до запуска государственной системы это единственный источник получения свободных образцов компьютерного почерка, без которых осложняется проведение идентификационных экспертных исследований. Помимо этого, такая деятельность компаний, аналогично личному использованию кейлоггеров, способствует прогрессу в данной области, позволяет говорить об актуальности, востребованности и развитии технологии.

Таким образом, мы представили возможные ответы на заявленные проблемные вопросы в сфере использования информации о компьютерном почерке пользователей. Однако их нельзя считать исчерпывающими и следует признать насущную потребность дальнейшего изучения данной темы различными научными коллективами.

В юридической среде компьютерный почерк – достаточно молодое явление, которое, в связи с этим, требует всестороннего изучения. Мы считаем, что информация о нём в условиях ускоряющейся цифровизации может стать незаменимой для раскрытия и расследования преступлений, заняв место сведений о традиционном рукописном почерке лица – экспертные исследования которого исторически носили весьма распространённый характер [40, с. 197; 41, с. 4]. Однако, чтобы такое использование стало возможным необходимо создать централизованную государственную систему (или выделить блок в существующей) для повсеместного сбора сведений о компьютерном почерке.

Так как человек сможет получить доступ к данным о скорости печати, динамике ввода, силе нажатия, временному интервалу между нажатиями клавиш и т. д., только будучи уполномоченным на то лицом и в ситуациях, где эта информация необходимо для решения государственных задач, а к государственным базам данных предъявляются повышенные требования по безопасности, можно говорить о том, что важнейшие права граждан на неприкосновенность их частной жизни и сохранения личной тайны будут соблюдены. Мы полностью разделяем позицию И. Ю. Остаповича и А. В. Нечкина, которые считают, что «новые проблемы, обусловленные особенностями реализации этих ценностей в интернете, требуют выработки наиболее эффективных механизмов их защиты в новых условиях реализации, а не полного отказа от них под предлогом их защиты» [29, с. 566].

Считаем, что при реализации описанной нами модели повсеместного сбора показателей компьютерного почерка вполне возможным будет сохранить указанный баланс между свободой и безопасностью, однако для этого необходима глубокая и детальная проработка всех возможностей и потенциальных рисков.

*Исследование выполнено за счёт гранта Российского научного фонда № 23-78-10011, https://rscf.ru/project/23-78-10011/*

## Библиография

1. Саликов М. С., Несмеянова С. Э., Колобаева Н. Е., Кузнецова С. С., Мочалов А. Н. Право на доступ в Интернет, анонимность и идентификация пользователей (конституционно-правовые проблемы) / под ред. М. С. Саликова. Екатеринбург:

Издательство УМЦ УПИ, 2020. 167 с.

2. Иванов В. В., Зуев Д. И. Цифровой двойники цифровая личность: понятие, соотношение, значение в процессе совершения киберпреступлений ив праве в целом // Правовое государство: теория и практика. 2022. № 4. С. 138–144. DOI: 10.33184/pravgos-2022.4.19.
3. Россинская Е. Р. О предмете и содержании учения об информационно-компьютерных криминалистических моделях компьютерных преступлений // Актуальные проблемы криминалистики и судебной экспертизы: Материалы Международной научно-практической конференции, Иркутск, 12 марта 2021 года. Иркутск: Восточно-Сибирский институт Министерства внутренних дел Российской Федерации, 2021. С. 167–171.
4. Уймин А. Г., Морозов И. М. Сравнительный анализ инструментов непрерывной онлайн-аутентификации и систем обнаружения аномалий для постоянного подтверждения личности пользователя // T-Comm: Телекоммуникации и транспорт. 2022. Т. 16. № 5. С. 48–55. DOI: 10.36724/2072-8735-2022-16-5-48-55.
5. Alenizi A., Al-Karaw Kh. A. Effective Biometric Technology Used with Big Data // Proceedings of Seventh International Congress on Information and Communication Technology. 2023. Pp. 239–250. DOI:10.1007/978-981-19-2394-4_22.
6. Syed Idrus S. Z. Soft Biometrics for Keystroke Dynamics. Computer Vision and Pattern Recognition. Universit´e de Caen Basse-Normandie, 2014. 134 p.;
7. Скуратов С. В. Использование клавиатурного почерка для аутентификации в компьютерных информационных системах // Безопасность информационных технологий. 2010. Т. 17. № 2. С. 35–38;
8. Ложников П. С., Сулавко А. Е. Применение сетей квадратичных форм для распознавания субъектов по динамическим биометрическим образам // Динамика систем, механизмов и машин. 2017. Т. 5. № 4. С. 77–84. DOI: 10.25206/2310-9793-2017-5-4-77-84.
9. Art_Andrei13. Мировой рынок биометрии: главные тренды // Хабр. Блог компании Digital Rights Center [Электронный ресурс]. 2022, 7 июня. URL: https://habr.com/ru/companies/digitalrightscenter/articles/670126/ (дата обращения: 06.08.2023).
10. Forsen G., Nelson M., Staron R. Jr. Personal attributes authentication techniques. Technical Report RADC-TR-77-333. Rome: Air Development Center, 1977. 333 p.
11. Аккаева Х. А. Проблемы использования современных биометрических технологий в информационно-поисковых системах регистрации граждан // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2014. № 4–1 (42). С. 13–16.
12. Расторгуев С. П. Программные методы защиты информации в компьютерах и сетях. М.: Издательство Агентства «Яхтсмен», 1993. 188 с.
13. Lv H.-R., Wang W.-Y. Biologic verification based on pressure sensor keyboards and classifier fusion techniques // IEEE Transactions on Consumer Electronics. 2006. Vol. 52 (3). Pp. 1057–1063.
14. Чевычелов И. Н., Калуцкий И. В. Обучение программной системы аутентификации на основе клавиатурного почерка // Современные инструментальные системы, информационные технологии и инновации: сборник научных трудов XII-ой Международной научно-практической конференции в 4-х томах, Курск, 19–20 марта 2015 года / Ответственный редактор: Горохов А. А. Том 4. Курск: Закрытое акционерное общество «Университетская книга», 2015. С. 240–242.

15. Сапиев А. З. Компьютерный почерк как способ идентификации пользователей в сети // Вестник Вологодского государственного университета. Серия: Технические науки. 2021. № 4 (14). С. 17–19.

16. Абзалов А. Р., Жиганов А. В., Самигуллина Р. Р. Аутентификация пользователей по клавиатурному почерку при использовании систем автоматического прокторинга // Национальные интересы: приоритеты и безопасность. 2020. Т. 16. № 3 (384). С. 582–596. DOI: 10.24891/ni.16.3.582.

17. Тарасова Л. В. Возможности подписи как биометрического метода аутентификации // Технологии XXI века в юриспруденции: Материалы Второй международной научно-практической конференции, Екатеринбург, 22 мая 2020 года / Под редакцией Д. В. Бахтеева. Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный юридический университет», 2020. С. 583–589.

18. Гришин И. Ю., Тимиргалеева Р. Р., Миронов М. В. Метод биометрической идентификации обучаемого в системах электронного образования // Современные информационные технологии и ИТ-образование: Сборник научных трудов II Международной научной конференции и XII Международной научно-практической конференции, Москва, 24–26 ноября 2017 года / Под редакцией В. А. Сухомлина. Москва: Лаборатория открытых информационных технологий факультета ВМК МГУ им. М. В. Ломоносова, 2017. С. 127–132.

19. Саликов М. С., Несмеянова С. Э., Колобаева Н. Е., Кузнецова С. С., Мочалов А. Н. Государственное регулирование Интернета и права человека / Под ред. д-ра юрид. наук, профессора М. С. Саликова. Екатеринбург: Издательство УМ УПИ, 2022. 220 с.

20. Маштанов П. Н., Мартынюк М. В. Обзор актуальных вопросов биометрической идентификации на основе особенностей клавиатурного почерка // Информационные системы и технологии ист-2021: сборник материалов XXVII Международной научно-технической конференции. Нижегородский государственный технический университет им. Р. Е. Алексеева, Нижний Новгород, 23–24 апреля 2021 года / Нижний Новгород: Нижегородский государственный технический университет им. Р. Е. Алексеева, 2021. С. 527–531.

21. Пащенко Д. В., Бальзанникова Е. А. Непрерывная идентификация пользователя по клавиатурному почерку с использованием представления на основе контекста состояний // XXI век: итоги прошлого и проблемы настоящего плюс. 2020. Т. 9. № 3 (51). С. 74–79. DOI: 10.46548/21vek-2020-0952-0012.

22. Соломатин М. С., Митрофанов Д. В. Использование методов биометрической аутентификации в автоматизированных системах управления с использованием клавиатурного почерка // Труды МАИ [сетевое научное издание]. 2020. № 114. URL: https://trudymai.ru/published.php?ID=119013. DOI: 10.34759/trd-2020-114-18.

23. Довгаль В. А. Обзор характеристик производительности наборов данных, используемых для обеспечения информационной безопасности на основе клавиатурного почерка // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2016. Выпуск 4 (191). С. 157–163.

24. Турутина Е. Э. Анализ методов электронной и биометрической аутентификации в системах контроля доступом // Вестник НЦБЖД. 2021. № 2 (48). С. 168–175.

25. Жуков М. Н. Обоснованность использования биометрических данных в криминалистической науке: История вопроса и проблемы правовой защиты персональных данных // Международный научно-исследовательский журнал. 2021.

№ 12–4 (114). С. 164–167.
26. Основы теории электронных доказательств: монография / под ред. докт. юрид. наук С. В. Зуева. М.: Юрлитинформ, 2019. 400 с.
27. Федоров И. З. К вопросу об установлении исполнителя электронного текста по клавиатурному почерку при раскрытии и расследовании преступлений // Вестник Барнаульского юридического института МВД России. 2019. № 2 (37). С. 113–116.
28. Фойгель Е. И. Современные тенденции и перспективы развития криминалистического учения о личности участников уголовного судопроизводства // Академический юридический журнал. 2023. Т. 24. № 1 (91). С. 101–108. DOI: 10.17150/1819-0928.2023.24(1).101-108.
29. Остапович И. Ю., Нечкин А. В. Реализация и защита прав человека в сети Интернет: проблемы соотношения и // Вестник Санкт-Петербургского университета. Право. 2022. Т. 13. № 2. С. 565–580. DOI: 10.21638/spbu14.2022.217.
30. Бахтеев Д. В. Искусственный интеллект в следственной деятельности: задачи и проблемы // Российский следователь. 2020. № 9. С. 3–6. DOI: 10.18572/1812-3783-2020-9-3-6.
31. Бессонов А. А. Некоторые перспективные направления дальнейшего развития российской криминалистики // Академическая мысль. 2019. № 3 (8). С. 22–27.
32. Крыжевич Л. С. Методы определения личности пользователя на основе индивидуальных особенностей компьютерного почерка // Вестник ВГУ. Серия: Системный анализ и информационные технологии. 2021. № 3. С. 47–58. DOI: 10.17308/sait.2021.3/3735.
33. Клавиатурный шпион кейлоггер (keylogger) на страже кибербезопасности предприятия // Bitcop [Электронный ресурс]. 2020, 3 апреля. URL: https://bitcop.ru/monitoring/keyloggers (дата обращения: 07.08.2023).
34. Monrose F., Rubin A. Authentication via Keystroke Dynamics / Proceedings of the Fourth ACM Conference on Computer and Communication Security. Apr 1, 1997. Zurich, Switzerland, Pp. 48–56.
35. Степенко В. Е., Богдановская А. Д. Биометрические персональные данные // Евразийский союз ученых. 2020. № 4–10 (73). С. 15–19.
36. Полуянова Е. В. Нормативное регулирование правоотношений, связанных с биометрическими персональными данными, в Российской Федерации // Вестник Владимирского юридического института. 2020. № 3 (56). С. 122–126.
37. Федотов Н. Н. Форензика – компьютерная криминалистика. М.: Юридический Мир, 2007. 432 с.
38. Бацких А. В., Дровникова И. Г., Зарубин В. С. Базовые аспекты модификации подсистем управления доступом к информации в автоматизированных системах органов внутренних дел на основе исследования клавиатурного почерка пользователей // Вестник Воронежского института МВД России. 2022. № 4. С. 21–32.
39. Wenxin Y., Xingshu Ch., Yi Zh. [et al]. HTTP Cookie Covert Channel Detection Based on Session Flow Interaction Features // Security and Communication Networks. 2023. Vol. 10. Pp. 1–16. DOI: 10.1155/2023/1348393.
40. Савкин А. А. Судебная почерковедческая экспертиза: важность и проблемы ее производства // Уголовная политика на современном этапе: Материалы Международной научно-практической конференции, проходившей в рамках II Байкальского юридического форума, Иркутск, 23–25 сентября 2021 года. Иркутск: Байкальский государственный университет, 2021. С. 194–199.
41. Баркова Т. В. Пути увеличения надежности экспертного вывода с использованием

современных технологий // Применение в юриспруденции современных технологий: актуальные вопросы теории и практики: Материалы Международной научно-практической конференции, Красноярск, 21 мая 2021 года. Красноярск: Красноярский государственный аграрный университет, 2021. С. 3–6.

## Результаты процедуры рецензирования статьи

*В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.*
*Со списком рецензентов издательства можно ознакомиться здесь.*

РЕЦЕНЗИЯ
на статью на тему «Сведения о компьютерном почерке: проблемы поиска баланса между свободой личности и безопасностью государства».

Предмет исследования.
Предложенная на рецензирование статья посвящена актуальным вопросам использования данных о личности, использованных в онлайн-ресурсах в целях обеспечения безопасности государства. Как указывает сам автор в своей статье, «Указанную задачу весьма успешно разрешают биометрические технологии, которые позволяют помимо этого повысить уровень личной информационной безопасности посредством настройки систем двухфакторной аутентификации для доступа в систему [4, с. 49]. Именно их исследование с позиций перспектив внедрения в общественную жизнь и является предметом настоящего исследования». В качестве конкретного предмета исследования выступили нормы законодательства, мнения учениях, эмпирические данные.

Методология исследования.
Цель исследования прямо в статье заявлена: «Целью настоящего исследования является доказать перспективность и допустимость с точки зрения соблюдения конституционных норм широкого распространения технологии идентификации и аутентификации пользователей компьютерных устройств на основе информации об их компьютерном (клавиатурном) почерке». Также обозначена методологическая основа: «были задействованы как общенаучные, так и специальные методы. Наиболее значимыми из всех явились: метод аналогии (при проецирование правовых режимов уже реализуемых биометрических систем на новые технологии), дедукция (при проецировании генеральных признаков биометрических данных на отдельные частные примеры), сравнительно-правовой (при сопоставлении законодательного регулирования биометрических данных в разных странах), системный (для согласования доктринальных и легальных подходов), метод моделирования (при конструировании возможных сценариев расширения числа применяемых в целях повышения государственной безопасности биометрических технологий) и др.».
В частности, автором используется совокупность общенаучных методов познания: анализ, синтез, аналогия, дедукция, индукция, другие. В частности, методы анализа и синтеза позволили обобщить и разделить выводы различных научных подходов к предложенной тематике, а также сделать конкретные выводы из эмпирических данных.
Наибольшую роль сыграли специально-юридические методы. В частности, автором активно применялся формально-юридический метод, который позволил провести анализ и осуществить толкование норм действующего законодательства (прежде всего, норм законодательства РФ). Например, следующий вывод автора: «Одним из правовых

механизмов, на которые мы указали в предыдущем пункте, может выступать детальное регулирование вопросов фиксации и использования сведений о компьютерном почерке. Для начала можно добавить упоминание о нём в ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», раскрыв наряду с остальными основными понятиями. Расширение сфер его применения может потребовать внесения соответствующих дополнений и в иные нормативно-правовые акты, существующего сегодня указания на существование компьютерного почерка исключительно в ГОСТах в скором времени будет недостаточно».

Таким образом, выбранная автором методология в полной мере адекватна цели исследования, позволяет изучить все аспекты темы в ее совокупности.

Актуальность.

Актуальность заявленной проблематики не вызывает сомнений. Имеется как теоретический, так и практический аспекты значимости предложенной темы. С точки зрения теории тема использования так называемого «цифрового следа» в целях обеспечения безопасности государства сложна и неоднозначна. Имеются как юридические, так и этические аспекты этой проблемы. Сложно спорить с автором в том, что «государство заинтересовано в максимальном контроле виртуальной среды. В частности, сохраняя право пользователей на анонимность, оно желает выработать механизм идентификации граждан, деанонимизации их личности в случае возникновения такой необходимости». При этом вопрос остается в том, не будут ли ограничены права и законные интересы самой личности в данном случае.

Тем самым, научные изыскания в предложенной области стоит только поприветствовать.

Научная новизна.

Научная новизна предложенной статьи не вызывает сомнений. Во-первых, она выражается в конкретных выводах автора. Среди них, например, такой вывод:

«В юридической среде компьютерный почерк – достаточно молодое явление, которое, в связи с этим, требует всестороннего изучения. Мы считаем, что информация о нём в условиях ускоряющейся цифровизации может стать незаменимой для раскрытия и расследования преступлений, заняв место сведений о традиционном рукописном почерке лица – экспертные исследования которого исторически носили весьма распространённый характер. Однако, чтобы такое использование стало возможным необходимо создать централизованную государственную систему (или выделить блок в существующей) для повсеместного сбора сведений о компьютерном почерке».

Указанный и иные теоретические выводы могут быть использованы в дальнейших научных исследованиях.

Во-вторых, автором предложены концептуальные идеи по формированию законодательства в заявленной сфере, что может быть полезно в правотворческой деятельности, а также специалистам в данной отрасли права.

Таким образом, материалы статьи могут иметь определенных интерес для научного сообщества с точки зрения развития вклада в развитие науки.

Стиль, структура, содержание.

Тематика статьи соответствует специализации журнала «Вопросы безопасности», так как она посвящена правовым проблемам, связанным с определением проблемы использования «цифрового следа» личности в целях обеспечения безопасности государства.

Содержание статьи в полной мере соответствует названию, так как автор рассмотрел заявленные проблемы, в целом достиг цели исследования.

Качество представления исследования и его результатов следует признать в полной мере положительным. Из текста статьи прямо следуют предмет, задачи, методология и основные результаты исследования.
Оформление работы в целом соответствует требованиям, предъявляемым к подобного рода работам. Существенных нарушений данных требований не обнаружено.

Библиография.
Следует высоко оценить качество использованной литературы. Автором активно использована литература, представленная авторами из России и из-за рубежа (Саликов М.С., Несмеянова С.Э., Колобаева Н.Е., Кузнецова С.С., Мочалов А.Н. Wenxin Y., Xingshu Ch., Yi Zh. и другие).
Таким образом, труды приведенных авторов соответствуют теме исследования, обладают признаком достаточности, способствуют раскрытию различных аспектов темы.

Апелляция к оппонентам.
Автор провел серьезный анализ текущего состояния исследуемой проблемы. Все цитаты ученых сопровождаются авторскими комментариями. То есть автор показывает разные точки зрения на проблему и пытается аргументировать более правильную по его мнению.

Выводы, интерес читательской аудитории.
Выводы в полной мере являются логичными, так как они получены с использованием общепризнанной методологии. Статья может быть интересна читательской аудитории в плане наличия в ней систематизированных позиций автора применительно к вопросам перспектив широкого распространения технологии идентификации и аутентификации пользователей компьютерных устройств на основе информации об их компьютерном (клавиатурном) почерке.

На основании изложенного, суммируя все положительные и отрицательные стороны статьи
«Рекомендую опубликовать»