Научная статья
УДК 343

РОЛЬ И ЗНАЧЕНИЕ ДЕАНОНИМИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ СЕТИ ИНТЕРНЕТ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Матросова Лидия Дмитриевна
Орловский юридический институт МВД России имени В. В. Лукьянова, Орел, Россия

itdovd@gmail.com

Аннотация. Цель статьи заключается в исследовании методов деанонимизации пользователей в сети Интернет. В работе рассматриваются современные подходы и технологии, используемые для идентификации личности пользователей на основе анализа различных цифровых следов, оставляемых ими в процессе сетевой активности. Особое внимание уделено методам, основанным на анализе поведения пользователей, их взаимодействии с различными онлайн-сервисами и контент-анализе публикаций. Автор подчёркивает важность значения деанонимизации пользователей сети Интернет. В заданном контексте доказано значение и роль данного процесса, а также предложен способ его совершенствования посредством инновационного открытия. Статья содержит обзор существующих научных исследований в области деанонимизации, а также рассматривает правовые аспекты данной проблемы, включая вопросы регулирования обработки персональных данных и ответственности за нарушение прав на конфиденциальность. Педставленный материал будет полезен для преподавателей и обучающихся, проводящих научные исследования в области информационного права.

Ключевые слова: информационные технологии, телекоммуникационные технологии, цифровизация, анонимность, деанонимизация, правоохранительные органы, сеть Интернет.

Для цитирования: Матросова Л. Д. Роль и значение деанонимизации пользователей сети Интернет в правоохранительной деятельности // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2025. № 2(103). С. 110–119.

THE ROLE AND IMPORTANCE OF DEANONYMIZATION OF INTERNET USERS IN LAW ENFORCEMENT

Lidiya D. Matrosova
Lukyanov Orel Law Institute of the Ministry of the Interior of Russia, Orel, Russia

itdovd@gmail.com

Annotation. The purpose of the article is to study the methods of deanonymization of users on the Internet. The paper examines modern approaches and technologies used to identify users based on the analysis of various digital footprints left by them in the process of network activity. Special attention is paid to methods based on the analysis of user behavior, their interactions with various online services and content analysis of publications. The authors analyze the importance of deanonymization of Internet users. In this context, the importance and role of this process is proved, as well as a way to improve it through innovative discovery is proposed. The article provides an overview of existing scientific

research in the field of deanonymization, as well as examines the legal aspects of this problem, including issues of regulating the processing of personal data and liability for violations of privacy rights. Thus, the presented material will be useful for teachers and students who have conducted scientific research in the field of information law.

Keywords: information technologies, telecommunication technologies, digitalization, anonymity, deanonymization, law enforcement agencies, the Internet.

For citation: Matrosova L. D. The role and importance of deanonymization of internet users in law enforcement // Scientific Bulletin of the Orel Law Institute of the Ministry of Internal Affairs of Russia named after V.V. Lukyanov. 2025. № 2(103). P. 110–119.

Повышение уровня развития цифровизации и информационных технологий является ключевым фактором реализации инновационной политики государства. Как совершенно точно подмечает В. В. Василенко, «в связи с этим многие исследователи и учёные сосредоточены на изучении влияния информационно-коммуникационных технологий на экономический рост и ускорение развития технологической сферы общества» [1, с. 101].

Одними из преимуществ информационно-телекоммуникационных технологий (ИТТ), привлекающих криминальные элементы, является возможность дистанционного совершения преступлений и сокрытие реальной личности субъекта преступления за цифровой личностью. По мере технологического развития информационных систем меняются установленные стандарты человеческой деятельности, их использование стало более необходимым не только в торговле и промышленности, но и в системе правоохранительных органов. Для идентификации личности интересующего объекта и получения о нём информации в настоящее время может эффективно использоваться *Open Source INTelligence* (далее – *OSINT*), представляющая собой комплекс разведывательно-аналитических средств и методов извлечения сведений из общедоступных ресурсов сети Интернет [2, с. 66].

Наиболее важной информацией, как замечает Поздышев Р. С., «в данном контексте представляется информация об адресах устройств, связанных с лицом, которым интересуется орган предварительного следствия, в сети Интернет (*ip-адресах*). Базовые методы работы с подобной информацией достаточно давно усвоены правоохранителями, однако, когда дело касается современных средств анонимизации личности в сети Интернет, возникают серьёзные и порой непреодолимые трудности» [3, с. 51].

В другом своём исследовании Поздышев Р. С. определяет, что «к основной сложности, с которой сталкиваются правоохранительные органы в данной сфере, следует отнести деанонимизацию пользователей компьютерных сетей. В данном контексте ключевой представляется информация об адресах устройств, связанных с пользователем, в сети Интернет (*ip-адресах*)» [4, с. 103].

В свою очередь Плешков В. Д. полагает, что «нарушители активно используют методы анонимизации для сокрытия следов своих преступлений. В связи с этим одной из крайне актуальных и перспективных задач компьютерной безопасности с точки зрения законодательства Российской Федерации становится способ идентификации пользователей сети Интернет. В ходе данного исследования был предложен и реализован один из методов решения проблемы деанонимизации пользователя мессенджеров» [5, с. 84].

Деанонимизация пользователей сети Интернет – это процесс, в ходе которого анонимные или псевдонимные данные пользователей становятся идентифицируемыми. В связи с чем можно выделить аспекты, которые подтверждают важнейшее значение исследования данной темы для правоохранительной деятельности.

Во-первых, деанонимизация позволяет правоохранительным органам выявлять и задерживать преступников, которые используют анонимность для совершения незаконных действий, таких как киберпреступления, торговля наркотиками, терроризм и другие виды преступлений.

Во-вторых, понимание методов деанонимизации помогает правоохранительным органам разрабатывать стратегии и технологии для мониторинга и анализа онлайн-активности, что способствует поддержанию общественного порядка.

В-третьих, деанонимизация может быть использована для сбора доказательств в судебных делах, где анонимные пользователи могут быть связаны с преступной деятельностью.

В-четвёртых, исследование деанонимизации помогает в анализе угроз, связанных с анонимными сетями и сервисами, такими как *Tor* или *Dark Web*, где преступные действия могут происходить под прикрытием анонимности.

В-пятых, исследование роли деанонимизации также поднимает важные вопросы о конфиденциальности, защите данных и прав человека, что требует от правоохранительных органов соблюдения баланса между безопасностью и правами граждан.

Так, изучив роль и значение деанонимизации пользователей сети Интернет для правоохранительной деятельности, считаем целесообразным предложить внедрять инновационные проекты, методы и способы. На наш взгляд, определённый интерес представляет изобретение, предложенное Бречко А. А., Булгаковой М. И. и Стародубцевым Ю. И., о способе деанонимизации пользователей сети Интернет [6]. Технический результат заключается в повышении надёжности деанонимизации пользователей сети Интернет. В способе транслируют мультимедиа-сообщения, смешанные с потоком данных, на одно или несколько электронных устройств, при этом поток данных содержит идентификатор, принимают на сервере идентификатор и данные по меньшей мере об одном устройстве связи, где в способе также принимают паразитное электромагнитное излучение, генерируемое электронным устройством при обработке мультимедиа- сообщения, смешанного с потоком данных, радиоприёмным модулем по меньшей мере на одном устройстве связи, затем извлекают идентификатор из принятого электромагнитного сигнала, после приёма сервером идентификатора и данных по меньшей мере об одном устройстве связи устанавливают личность пользователя.

Как справедливо отмечают Иванов И. И. и Кондрат И. Н., проблемная ситуация внедрения искусственного интеллекта в криминалистическое изучение преступной деятельности сегодня характеризуется рядом факторов. Один из которых – неудовлетворительный уровень технического оснащения подразделений, специализирующихся на расследовании киберпреступлений и сложность идентификации преступников в случаях, когда преступление совершено с использованием незащищённой сети передачи данных [7, с. 8].

Изобретение относится к области идентификации пользователей сети, в частности их деанонимизации. Средство обеспечения анонимности – это программное/программно-аппаратное средство, обеспечивающее сокрытие идентификационных данных пользователя (потребителя) какого-либо ресурса в сети Интернет, при этом идентификационные данные включают, но не ограничиваются персональными данными пользователя, IP-адресом, настройками браузера, идентификатором в сети провайдера.

На сегодняшний день одной из основных проблем как в организационном, тактическом, техническом, так и правовом аспектах можно считать проблему деанонимизации пользователя сети Интернет. Под понятием деанонимизации

пользователя сети Интернет понимается комплекс мероприятий, направленный на установление его личности. При этом пользователь сети Интернет [в контексте способа] рассматривается как лицо, совершающее противоправные деяния в киберпространстве.

Известен способ деанонимизации пользователей сети Интернет, заключающийся в том, что в сетях с низкой задержкой передачи (т. е. в сетях *Tor* и *VPN*) пользователя идентифицируют за счёт корреляции времени прохождения пакетов. Недостатком данного способа является сложность реализации и низкая эффективность из-за необходимости одновременного контроля большого числа узлов сети связи.

Можно выделить ещё один способ деанонимизации пользователей сети Интернет, который заключается в том, что пользователя идентифицируют за счёт собираемых характеристик электронного устройства (*ip-адрес*, *MAC-адрес*, значения настроек и т. д.). Недостатком этого способа является низкая эффективность из-за слабой корреляции собираемых данных с личностью пользователя. Наиболее близким по технической сущности и выполняемым функциям к заявленному (прототипом) является «Способ кросс-девайс таргетинга пользователей», заключающийся в том, что транслируют мультимедиа-сообщения, смешанные с потоком аудиоданных на одно или несколько электронных устройств, при этом поток аудиоданных содержит идентификатор, принимают поток аудиоданных по меньшей мере на одном устройстве связи, извлекают идентификатор из принятого потока аудиоданных, принимают на сервере идентификатор и данные по меньшей мере об одном устройстве связи, отправляют одно или более сообщений по меньшей мере на одно устройство связи, связанное с идентификатором. При этом идентификатор, содержащийся в потоке аудиоданных, может быть как в слышимом, так и в неслышимом диапазоне частот. Техническая проблема состоит в необходимости расширения арсенала технических средств деанонимизации.

Техническая проблема обусловлена ограниченностью применения существующих средств деанонимизации. Техническим результатом является расширение арсенала технических средств деанонимизации. Поэтому любая техническая проблема расширения арсенала технических средств деанонимизации пользователей сети Интернет устраняется за счёт создания технического решения, заключающегося в использовании дополнительного идентификатора, извлекаемого из паразитного электромагнитного излучения (ЭМИ) электронного устройства, при этом излучение принимается на радиомодуль устройства связи, идентифицированного относительно личности владельца. Указанная проблема, по нашему мнению, решается таким образом, что в способе деанонимизации пользователей сети Интернет транслируют мультимедиа-сообщения, смешанные с потоком данных, на одно или несколько электронных устройств, при этом поток данных содержит идентификатор, принимают на сервере идентификатор и данные по меньшей мере об одном устройстве связи, согласно изобретению дополнительно принимают паразитное ЭМИ, генерируемое электронным устройством при обработке мультимедиа-сообщения, смешанного с потоком данных, радиоприёмным модулем по меньшей мере на одном устройстве связи, затем извлекают идентификатор из принятого электромагнитного сигнала, после приёма сервером идентификатора и данных по меньшей мере об одном устройстве связи устанавливают личность пользователя. Паразитное ЭМИ – это нежелательное электромагнитное излучение, которое возникает в результате работы различных электронных компонентов внутри устройства. Например, такие излучения могут возникать от микропроцессоров, видеокарт, антенн и других элементов при их функционировании. Таким образом, речь идёт о процессе, когда электронные устройства могут случайно принимать нежелательные сигналы, вызванные работой

мультимедийных приложений, и смешивать их с основными данными, передаваемыми по беспроводному каналу.

Проведённый нами анализ уровня техники позволил установить, что аналоги, характеризующиеся совокупностями признаков, тождественными всем признакам заявленного способа, отсутствуют. Следовательно, заявленное изобретение соответствует такому условию патентоспособности, как «новизна». Перечисленная новая совокупность существенных признаков обеспечивает расширение возможностей способа прототипа за счёт использования электронного устройства в качестве радиопередатчика, транслирующего в радиоэфир идентификатор, который принимает устройство связи, находящееся в непосредственной близости к электронному устройству.

Результаты поиска известных решений в данной и смежной областях использования техники с целью выявления признаков, совпадающих с отличительными от прототипов признаками заявленного изобретения, показали, что они являются уникальными, не похожи на уже известные разработки и не являются очевидным развитием существующих технологий. Из определённого заявителем уровня техники не выявлена известность влияния предусматриваемых существенными признаками заявленного изобретения на достижение указанного технического результата. Следовательно, заявленное изобретение соответствует условию патентоспособности «изобретательский уровень». «Промышленная применимость» способа обусловлена наличием элементной базы, на основе которой могут быть выполнены устройства, реализующие данный способ с достижением указанного в изобретении результата.

Заявленный способ поясняется тем, что в качестве устройства трансляции мультимедиа-сообщений выступает любой ресурс в сети Интернет, например сайт. При этом транслируемые сообщения предварительно смешивают с данными, при обработке которых на электронном устройстве пользователя сети Интернет возникают паразитные ЭМИ с заданными параметрами. Идентификатор представляет собой некоторое число, связанное на стороне сервера с конкретным электронным устройством, которое получало мультимедиа-сообщения. В качестве приёмника транслируемых мультимедиа-сообщений может выступать любое электронное устройство, например ПЭВМ. При этом доступ пользователя сети Интернет к транслируемым сообщениям осуществляется с помощью средств обеспечения анонимности, например сети *Tor*.

В настоящее время актуальным для расследования преступлений, связанных с использованием телекоммуникационных технологий, являются технологии обработки электромагнитных излучений (ЭМИ), возникающих при работе электронных устройств. В данном случае речь идёт о ситуации, когда устройство связи принимает нежелательные (паразитные) сигналы, возникающие при передаче или обработке мультимедийной информации. Эти сигналы могут смешиваться с основным потоком данных, передаваемых через радиоприёмный модуль устройства.

Можно выделить некоторые технические процессы, включающие несколько блоков, связанных с обработкой сигналов и данных.

Блок 1 содержит электронное устройство, которое занимается обработкой мультимедийных сообщений. Это может быть любое устройство, связанное с цифровыми технологиями, такими как компьютеры, смартфоны, серверы и т. п., работающие с аудио-, видео- или графическими файлами. Когда такое устройство обрабатывает мультимедийный контент (например, кодирует видео, отправляет или принимает медиафайлы), оно генерирует электромагнитные излучения (ЭМИ), поскольку его компоненты (процессоры, схемы, память и т. д.) работают на высоких частотах.

Блок 2 отвечает за приём электромагнитных волн, которые возникают как результат обработки мультимедийных данных. Паразитное ЭМИ, генерируемое первым блоком, попадает сюда вместе с полезным сигналом (потоком данных). Такой приёмник может находиться на другом электронном устройстве или в пределах одного устройства, где происходят другие процессы обработки данных. То есть второй блок фиксирует ЭМИ-сигнал, который является результатом функционирования первого блока, но этот сигнал не несёт полезной информации, он считается паразитным шумом, мешающим нормальной работе.

В правоохранительных органах используется основной полезный сигнал, передаваемый между устройствами. Например, это может быть передача файлов по сети, обмен информацией между узлами или работа программного обеспечения. Однако в этом потоке также присутствуют нежелательные электромагнитные колебания (паразитное ЭМИ), вызванные работой электронного оборудования.

Основными целями применения такой системы являются:

– мониторинг паразитных излучений. Возможно, система предназначена для анализа или измерения уровня электромагнитных помех, создаваемых электронными устройствами. Это важно для разработки методов снижения влияния паразитных ЭМИ на работу устройств;

– использование паразитного ЭМИ для диагностики. Иногда ЭМИ может использоваться для оценки состояния электроники. Некоторые неисправности в оборудовании могут вызывать необычные виды электромагнитных излучений, которые можно использовать для диагностики проблем;

– защита от несанкционированного перехвата данных. Паразитное ЭМИ также может нести информацию о передаваемом сигнале, поэтому изучение этих колебаний иногда используется для защиты передачи данных от утечек.

В блоке 1 принимают паразитное ЭМИ, генерируемое электронным устройством при обработке мультимедиа-сообщения, смешанного с потоком данных, радиоприёмным модулем по меньшей мере на одном устройстве связи. Устройство связи [в контексте способа] – программно-аппаратное устройство, предназначенное для работы в сетях сотовой связи. При этом современные устройства связи, помимо основного радиоприёмного модуля, обеспечивающего функционирование устройства по прямому назначению, как правило, имеют другие радиоприёмные модули, например: модуль *Bluetooth*, модуль *Wi-Fi* или FM-приёмник.

В блоке 2 извлекают идентификатор из принятого электромагнитного сигнала. Под извлечением идентификатора из паразитного ЭМИ понимается выявление изменения по известному шаблону любого из параметров принятого радиосигнала, например амплитуды демодулированного сигнала при настройке радиоприемного модуля на заданную частоту. После извлечения идентификатора информацию и данные об устройстве связи, радиомодулем которого было принято паразитное ЭМИ, отправляют на сервер. Данные об устройстве связи представлены, но не ограничены mac-адресом, номером IMEI, номером телефона. Идентификатор и данные об устройстве связи отправляют известными способами через сеть Интернет с помощью предустановленного на устройстве программного обеспечения или посредством способов удалённого управления устройством, предусмотренных стандартом GSM.

В блоке 3 принимают на сервере идентификатор и данные по меньшей мере об одном устройстве связи. Приём осуществляется известными способами.

В блоке 4 устанавливают личность пользователя сети Интернет. Личность пользователя устанавливается при помощи сопоставления полученного идентификатора с данными об устройстве связи, идентифицированном относительно личности владельца, который одновременно является пользователем сети Интернет.

Например, в соответствии с Федеральным законом «О связи» для получения идентификационного электронного модуля абонента (SIM-карта) необходимо предоставление оператору связи паспортных данных абонента[1]. Также операторы связи хранят объём информации, достаточный для установления личности пользователя по данным об устройстве связи, в том числе паспортные данные пользователя, текстовые сообщения, направления вызовов, данные о местоположении[2]. При этом предполагается, что устройство связи не используется для совершения противоправных действий, зарегистрировано на пользователя и функционирует без использования средств обеспечения анонимности.

Таким образом, идентификатор, отправленный вместе с мультимедиа-сообщением на электронное устройство, через которое осуществляется анонимный доступ к ресурсу в сети Интернет, подвергаясь обработке электронным устройством, излучается в радиоэфир в виде паразитного ЭМИ. При этом идентификатор принимается радиоприёмным модулем устройства связи, а устройство связи, идентифицированное относительно личности пользователя, отправляет на сервер вместе с идентификатором данные об устройстве связи, при этом на сервере устанавливается личность пользователя путём сопоставления идентификатора и данных об устройстве связи. Следовательно, представленная совокупность существенных признаков достаточна для решения проблемы и достижения технического результата.

Исследуемый способ деанонимизации пользователей сети Интернет заключается в том, что транслируют мультимедиа-сообщения, смешанные с потоком данных, на одно или несколько электронных устройств, при этом поток данных содержит идентификатор, принимают на сервере идентификатор и данные по меньшей мере об одном устройстве связи, отличающийся тем, что принимают паразитное электромагнитное излучение, генерируемое электронным устройством при обработке мультимедиа-сообщения, смешанного с потоком данных, радиоприёмным модулем по меньшей мере на одном устройстве связи, затем извлекают идентификатор из принятого электромагнитного сигнала, после приёма сервером идентификатора и данных по меньшей мере об одном устройстве связи устанавливают личность пользователя.

Как справедливо отмечает Шумилин В. П., «залог успеха деятельности любых подразделений правоохранительной системы в большинстве своём зависит от степени систематизированности информации о совершённых в прошлом преступлениях, причастных к преступлениям лицах, средствах и формах их совершения, различных следах на месте преступления и объектах криминального характера, а также от возможности и умения сотрудника ОВД пользоваться подобными банками данных в своей повседневной деятельности для выявления, розыска и отождествления интересующих его явлений и объектов» [8, с. 174].

По нашему мнению, современные технологии позволяют правоохранительным органам эффективно идентифицировать преступников в интернете, используя широкий спектр инструментов – от анализа сетевого трафика до сотрудничества с провайдерами и социальными платформами. Примеры конкретных дел и судебных решений служат ярким доказательством эффективности этих методов. Однако работа оставляет открытым вопрос о потенциальных злоупотреблениях властью и риске нарушения

[1] О связи : Федер. закон Рос. Федерации от 7 июля 2003 г. № 126-ФЗ // Рос. газ. 2003.10 июл. № 135.
[2] Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи: постановление Правительства Рос. Федерации от 12 апреля 2018 г. № 445 // Собр. законодательства Рос. Федерации. 2018, № 17, ст. 2489.

конституционных прав граждан. В этой связи авторы предлагают ряд рекомендаций по совершенствованию законодательства и внедрению механизмов контроля над деятельностью правоохранительных органов в сфере цифровой идентификации. Таким образом, исследование деанонимизации пользователей в интернете является важным аспектом для эффективной работы правоохранительных органов и обеспечения безопасности общества.

Современные технологии предоставляют правоохранительным органам целый арсенал инструментов для идентификации преступников в интернете. Отметим несколько ключевых направлений, где цифровые методы помогают в этой работе:

1. Анализ сетевого трафика – правоохранительные органы используют специализированные системы мониторинга трафика для отслеживания подозрительных действий в сети. Эти инструменты позволяют анализировать данные, передаваемые через интернет, включая IP-адреса, метаданные и другие технические характеристики соединений. Это помогает выявлять хакеров, мошенников и иных злоумышленников, действующих в киберпространстве.

2. Использование технологий *Big Data* – большие объёмы данных собираются и обрабатываются системами анализа больших данных (*Big Data*). Эти системы позволяют находить скрытые связи между различными источниками информации, такими как аккаунты социальных сетей, электронные письма, банковские транзакции и др., что значительно упрощает процесс расследования преступлений.

3. Киберполиция и сотрудничество с IT-компаниями – взаимодействие правоохранительных органов с крупными технологическими компаниями играет важную роль в борьбе с киберпреступностью. Социальные платформы, такие как *Facebook, Twitter, VKontakte*, активно сотрудничают с полицией, предоставляя доступ к данным пользователей, если есть подозрения в нарушении закона. Это способствует быстрой блокировке вредоносной активности и идентификации нарушителей.

4. Цифровые отпечатки (*Digital Footprints*) – каждое устройство оставляет уникальный цифровой след в интернете – от IP-адресов до файлов *cookie*. Анализируя эти следы, правоохранители могут отслеживать действия конкретного лица даже в условиях анонимизации. Например, использование VPN-сервисов и прокси-серверов усложняет идентификацию, но современные технологии позволяют связывать активности различных устройств и учётных записей, восстанавливая цепочку действий преступника.

5. Децентрализованные и зашифрованные сети – несмотря на сложность работы с такими технологиями, как *Tor* и криптовалюты, правоохранительные органы разрабатывают новые способы отслеживания и деанонимизации участников подобных сетей. Использование специальных алгоритмов машинного обучения и методов анализа графов позволяет устанавливать взаимосвязь между пользователями и их действиями.

Все эти технологии вместе создают мощную систему защиты правопорядка в цифровом пространстве. Благодаря сотрудничеству между государственными органами, техническими компаниями и аналитиками правоохранительные структуры получают возможность оперативно реагировать на преступления в интернете и предотвращать их повторение.

---

1. Матросова Л. Д. Цифровые технологии в реализации конституционного права граждан на информацию // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2024. № 2(99). С. 98–106.
2. Матросова Л. Д., Кислицин И. А. Инструменты для поиска оперативно-значимой информации по открытым источникам // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2022. № 4(93). С. 65–72.

3. Патент № 2782705 C1 Российская Федерация, МПК H04N 21/25, H04L 61/00. способ деанонимизации пользователей сети Интернет : № 2021138281 : заявл. 22.12.2021 : опубл. 01.11.2022 / А. А. Бречко, М. И. Булгакова, Ю. И. Стародубцев [и др.] ; заявитель Федеральное государственное казенное военное образовательное учреждение высшего образования Академия Федеральной службы охраны Российской Федерации.
4. Плешков В. Д. Разработка программного комплекса по деанонимизации пользователей сети Интернет // Инновационные технологии в подготовке современных профессиональных кадров: опыт, проблемы : сборник научных трудов, Челябинск, 30 января 2023 года. Челябинск: Челябинский филиал федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», 2023. С. 83–88.
5. Поздышев Р. С. Активная деанонимизация личности преступника в сети интернет с использованием canarytokens // Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. 2024. № 1(69). С. 101–106.
6. Поздышев Р. С. Деанонимизация личности преступника в сети Интернет // Вестник Уральского юридического института МВД России. 2022. № 2(34). С. 50–53.
7. Иванов И. И., Кондрат И.Н. Особенности предупреждения преступлений, совершенных с использованием современных информационно-телекоммуникационных технологий // Мировой судья. 2024. № 12. С. 2–9.
8. Шумилин В. П. Система информации и информационное обеспечение управления в правоохранительных органах // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2018. № 4(77). С. 173–176.

1. Matrosova L. D. Cifrovy`e texnologii v realizacii konstitucionnogo prava grazhdan na informaciyu // Nauchny`j vestnik Orlovskogo yuridicheskogo instituta MVD Rossii imeni V.V. Luk`yanova. 2024. № 2(99). S. 98–106.
2. Matrosova L.D., Kislicin I.A. Instrumenty` dlya poiska operativno-znachimoj informacii po otkry`ty`m istochnikam // Nauchny`j vestnik Orlovskogo yuridicheskogo instituta MVD Rossii imeni V.V. Luk`yanova. 2022. № 4(93). S. 65–72.
3. Patent № 2782705 C1 Rossijskaya Federaciya, MPK H04N 21/25, H04L 61/00. sposob deanonimizacii pol`zovatelej seti Internet : № 2021138281 : zayavl. 22.12.2021 : opubl. 01.11.2022 / A. A. Brechko, M. I. Bulgakova, Yu. I. Starodubcev [i dr.] ; zayavitel` Federal`noe gosudarstvennoe kazennoe voennoe obrazovatel`noe uchre-zhdenie vy`sshego obrazovaniya Akademiya Federal`noj sluzhby` oxrany` Rossijskoj Fe-deracii.
4. Pleshkov V. D. Razrabotka programmnogo kompleksa po deanonimizacii pol`zo-vatelej seti Internet // Innovacionny`e texnologii v podgotovke sovremenny`x pro-fessional`ny`x kadrov: opy`t, problemy` : sbornik nauchny`x trudov, Chelyabinsk, 30 yan-varya 2023 goda. – Chelyabinsk: Chelyabinskij filial federal`nogo gosudarstvennogo byudzhetnogo obrazovatel`nogo uchrezhdeniya vy`sshego obrazovaniya «Rossijskaya akademiya narodnogo xozyajstva i gosudarstvennoj sluzhby` pri Prezidente Rossijskoj Federacii», 2023. S. 83–88.
5. Pozdy`shev R. S. Aktivnaya deanonimizaciya lichnosti prestupnika v seti inter-net s ispol`zovaniem canarytokens // Vestnik Vserossijskogo instituta povy`sheniya kvalifikacii sotrudnikov Ministerstva vnutrennix del Rossijskoj Federacii. 2024. № 1(69). S. 101–106.
6. Pozdy`shev R. S. Deanonimizaciya lichnosti prestupnika v seti Internet // Vestnik Ural`skogo yuridicheskogo instituta MVD Rossii. 2022. № 2(34). S. 50–53.

7. Ivanov I.I., Kondrat I.N. Osobennosti preduprezhdeniya prestuplenij, sover-shenny`x s ispol`zovaniem sovremenny`x informacionno-telekommunikacionny`x tex-nologij // Mirovoj sud`ya. 2024. № 12. S. 2–9.
8. Shumilin, V. P. Sistema informacii i informacionnoe obespechenie upravle-niya v pravooxranitel`ny`x organax // Nauchny`j vestnik Orlovskogo yuridicheskogo in-stituta MVD Rossii imeni V.V. Luk`yanova. 2018. № 4(77). S. 173–176.

Информация об авторе

Лидия Дмитриевна Матросова. Начальник кафедры информационных технологий в деятельности органов внутренних дел, кандидат юридических наук, доцент.
Орловский юридический институт МВД России имени В.В. Лукьянова
302027, Россия, г. Орел, ул. Игнатова, 2.

Information about the author

Lidya D. Matrosova. Chief of the Department of Information technologies in Ministry of Internal Affairs. Candidate of Law, Associate Professor.
Lukyanov Orel Law Institute of the Ministry of the Interior of Russia.
302027, Russia, Orel, Ignatova Str., 2.

Статья поступила в редакцию 30.03.2025; одобрена после рецензирования 20.05.2025; принята к публикации 17.06.2025.
The article was received in the editorial office on 30.03.2025; approved after review on 20.05.2025; accepted for publication on 17.06.2025.