Научная статья
УДК 343.97

ОСОБЕННОСТИ ПОЗНАНИЯ АЛГОРИТМИЗАЦИИ СЕТИ «ДАРКНЕТ» КАК ИСТОЧНИКА КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Александр Иозосович Милюс
Восточно-Сибирский институт МВД России, г. Иркутск, Российская Федерация, milyus.ai@mail.ru

Аннотация. Важным условием результативного расследования преступлений, связанных с информационно-телекоммуникационными технологиями, становится обязательное наличие дополнительных знаний в области информатики. Однако не во всех случаях субъект расследования обладает необходимыми глубокими знаниями, позволяющими оперативным образом реагировать на складывающуюся следственную ситуацию.

В статье рассматриваются некоторые алгоритмы сокрытия следов преступления в интерактивной среде – интернете, а также возможные способы минимизации негативного влияния феномена анонимности для процесса расследования, что в свою очередь позволяет качественным образом обеспечить реализацию процесса предварительного расследования преступлений, связанных с информационно-телекоммуникационными технологиями. Автором обозначены основные понятия и алгоритмы при работе с данными в информационной среде в режиме анонимности, зная о которых, субъект расследования может эффективным образом распределять силы и средства при расследовании преступлений, связанных с использованием интерактивных информационных ресурсов. Предложенные рекомендации могут быть использованы правоохранительными органами в правоприменительной практике для повышения качества проводимого расследования.

Ключевые слова: информация, доказательства, даркнет, темный интернет, шифрование, криптография, передача данных, браузер, источник информации, средства коммуникации

Для цитирования: Милюс А. И. Особенности познания алгоритмизации сети «Даркнет» как источника криминалистически значимой информации при расследовании преступлений, совершенных с использованием информационно-коммуникационных технологий // Криминалистика: вчера, сегодня, завтра. 2025. Т. 36. № 24. С. 162–173.

FEATURES OF KNOWLEDGE OF THE ALGORITHMIZATION OF THE DARKNET NETWORK AS A SOURCE OF FORENSIC SIGNIFICANT INFORMATION IN THE INVESTIGATION OF CRIMES COMMITTED USING INFORMATION AND COMMUNICATION TECHNOLOGIES

Alexander I. Milius
East Siberian Institute of the MIA of Russia, Irkutsk, Russian Federation, milyus.ai@mail.ru

Abstract. For the successful investigation of crimes involving information and telecommunications technologies, a deep understanding of computer science is essential. However, not all investigators have the requisite specialized knowledge to swiftly address changing investigative scenarios.

This article explores various algorithms for concealing criminal evidence in the interactive digital environment, specifically the internet, and discusses strategies to mitigate the adverse effects of anonymity on investigations. This enables the efficient conduct of preliminary probes into crimes related to information and telecommunications technologies. The author presents crucial concepts and algorithms for managing data in an anonymized digital context. Familiarity with these principles empowers investigators to allocate resources effectively when examining crimes that involve interactive digital platforms. The suggested recommendations can be applied by law enforcement agencies to enhance the quality of their investigative processes.

Keywords: information, evidence, darknet, dark internet, encryption, cryptography, data transfer, browser, information source, communication tools

For citation: Milius A. I. Osobennosti poznaniya algoritmizatsii seti «Darknet» kak istochnika kriminalisticheski znachimoy informatsii pri rassledovanii prestupleniy, sovershennykh s ispol'zovaniyem informatsionno-kommunikatsionnykh tekhnologiy [Features of knowledge of the algorithmization of the darknet network as a source of forensic significant information in the investigation of crimes committed using information and communication technologies]. Kriminalistika: vchera, segodnya, zavtra = Forensics: yesterday, today, tomorrow. 2025, vol. 36 no. 4, pp. 162–173 (in Russ.).

Введение

Расследование преступлений является одним из приоритетных направлений деятельности МВД России. В последние годы активное распространение получили преступления, совершенные с использованием информационно-телекоммуникационных технологий (далее по тексту ИТТ), к которым относятся не только преступления, предусмотренные ст. 272–274 УК РФ, но и так называемые дистанционные мошенничества и иные формы хищения имущества граждан, при совершении которых так или иначе применялись ИТТ. Помимо этого, в современных условиях при совершении других преступлений все чаще находят свое отражение применяемые информационные технологии. В связи с этим президент Российской Федерации В. В. Путин на расширенном заседании коллегии МВД России, состоявшейся в 2025 году, указал на необходимость обращения дополни-

тельного внимания на раскрываемость преступлений, совершённых с использованием информационных технологий[1]. Обращение главы государства вполне обосновано и логично, так как в 2024 году в России было зарегистрировано 765,4 тысяч преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что составляет около 40% от общего числа зафиксированных преступлении[2]. Приведенные статистические данные свидетельствуют о том, что сфера ИТТ, являясь динамично и активно развивающейся, представляет собой весьма привлекательное направление для лиц, осуществляющих противоправную (криминальную) деятельность. Причин, влияющих на активное распространение указанных преступлений, достаточно много, однако к основным из них следует отнести активное развитие науки и техники, возросший ритм жизни, а также информационную неосведомленность населения.

Основная часть

Для понимания механизма совершения преступления (подготовки, совершения, сокрытия) субъекту расследования необходимо иметь определенные знания о способах совершения преступлений, механизме следообразования, а также общей концепции использования телекоммуникационных систем и их роли в совершении преступления. В связи с этим справедливым является утверждение профессора О. П. Грибунова о том, что «изучение способов преступления способствует решению поисковых задач» [1, с. 1102]. Действительно, если субъект расследования осведомлен о том, что именно ему необходимо установить (выяснить), каким образом осуществлять поисковые мероприятия и в каких границах, то деятельность по сбору, оценке и анализу доказательств становится кратно эффективнее, чем в том случае, если он работает в условиях недостаточности понимания проведения необходимых мероприятий. Для качественной и всесторонней реализации процесса расследования по преступлению, целесообразным является изучение общей архитектоники работы с информацией в сфере телекоммуникационных технологий и алгоритмов цифрового следообразования. Именно поэтому «для развития методик расследования преступлений, связанных с применением ИТТ, следует учитывать темпы развития информационных технологий» [2, с. 199], что даст возможность рациональным образом реагировать на криминальное поведение преступников.

Одним из направлений, которое необходимо изучить субъекту расследования для эффективного и качественного осуществления расследования таких преступлений, является шифрование данных, которое не позволит неподготовленному человеку понять определенный массив информационных данных, а также предпринять меры по их фиксации и изъятию.

Шифрование, если говорить простым языком, – это технология кодирования и раскодирования данных. История шифрования насчитывает более 4 тысяч лет и берет свое начало в Древнем Египте, когда для шифрования использовали замену общепринятых иероглифов на иные сим-

[1] Расширенное заседание коллегии МВД [Электронный ресурс]. – URL: http://www.kremlin.ru/events/president/news/76408 (дата обращения 24.03.2025).

[2] МВД России публикует статистическую информацию о состоянии преступности в Российской Федерации за 2024 год [Электронный ресурс]. – URL: https://mvdmedia.ru/news/official/mvd-rossii-publikuet-statisticheskuyu-informatsiyu-o-sostoyanii-prestupnosti-v-rossiyskoy-federatsii2024/

волы и знаки. Однако, если обратиться к научному толкованию данной дефиниции, то под шифрованием понимается применение определенного алгоритма кодирования данных, направленного на невозможность их понимания для дальнейшего чтения. Говоря о шифровании, нельзя не упомянуть и о криптографии (в переводе с древнегреческого «тайнопись») – науке о математических методах обеспечения шифрования данных. Именно благодаря криптографии стало возможным создавать математические модели и автоматизировать процессы шифрования и последующего дешифрования данных, которые в настоящее время достигли высокого уровня и применяются в разнообразных сферах: от обычного общения в мессенджерах до засекреченных каналов связи международного уровня.

Наличие защиты от свободного (беспрепятственного) доступа со стороны иных лиц к массиву данных позволяет преступникам обеспечить безопасный обмен данными, поиск интересующей информации, а также изучать и анализировать информацию в условиях анонимности. В связи с этим А. А. Рудых справедливо отмечает, что «на сегодняшний день самая ценная для раскрытия преступления информация все чаще находится в зашифрованном виде» [3, с. 205], и именно поэтому защищенные путем шифрования данные относительно совершенного преступления представляют особый интерес для субъекта расследования, так как именно в них зачастую содержатся криминалистически значимые сведения о совершенном преступлении. Такие данные в последующем могут выступать в качестве доказательств. Профессор Д. А. Степаненко предлагает именовать такие доказательства электронно-цифровыми и подразумевает под этим понятием такие сведения, которые получены в электронном виде и подтверждают факты и обстоятельства, связанные с делом [4, с. 24]. Не вдаваясь в полемику относительно дефиниции обозначения таковых доказательств, отметим важность их фактического наличия и изучения субъектом расследования, для чего крайне важным представляется уяснение сути шифрования данных.

Обращаясь к вопросу совершения преступлений с использованием ИТТ, важно отметить, что использование цифровых данных зачастую находит свое отражение при подготовке, совершении и сокрытии преступления. Так, на этапе подготовки к совершению преступления преступник осуществляет поиск информации и осуществляет координацию действий со своими сообщниками, подыскивает средства связи, которые оснащены функциями шифрования, использует электронно-вычислительную технику для хранения информации. Используя полученную на подготовительном этапе информацию, преступник коммуницирует с потерпевшим или иными лицами с помощью информационных технологий, позволяющих скрыть или видоизменить цифровые следы. А после совершения преступления предпринимает действия, направленные на безвозвратное модифицирование или защиту криминалистически значимой электронно-цифровой информации при помощи специальных алгоритмов шифрования либо специализированного программного обеспечения.

Одним из наиболее распространенных способов минимизации оставляемых цифровых следов присутствия в виртуальной информационной среде является так называемый «Темный интернет». Так, пожалуй, не найдется человека, который не слышал бы слова «Даркнет» («DarkNet»), которое дословно может

быть переведено с английского языка, как «скрытая сеть», «тёмный интернет», «тёмная сеть», «теневая сеть», «тёмный веб». Однако разнообразные названия не меняют единственной сути – это информационный ресурс, обеспечивающий максимально возможный конфиденциальный канал связи между абонентами. Если рассматривать «Даркнет» в более широком смысле, то следует отметить, что он представляет собой скрытую информационную сеть, обмен данными по которой возможен только между определёнными узлами (пирами – пользователями, которые участвуют в передаче файлов или информации) при использовании нестандартизированных транспортных протоколов данных (TCP – Transmission Control Protocol). Так, информационные данные (интернет-страницы, изображения, звуковые и видеофайлы и др.), которые не имеют возможности быть верифицированными стандартным программным обеспечением (в том числе поискового характера), представляют собой «теневую» сторону интернета. Таким образом, цифровые следы присутствия пользователя, который готовится к совершению преступления, совершает или активным образом скрывает его, минимизируются, что обусловлено шифрованием данных, перенаправлением потоков данных и иными способами, которые позволяют весьма длительное время оставаться пользователю незамеченным в виртуальном пространстве.

Безусловно, выявление и пресечение работы подобных ресурсов активным образом осуществляется правоохранительными органами, однако невозможно оперативно реагировать на их деятельность ввиду их многочисленности и скрытного характера функционирования, а также отсутствия объективной возможности мониторинга значительных информационных массивов данных.

Кроме того, в настоящее время широкое распространение получил сервис VPN («virtual private network»), что в переводе с английского означает «виртуальная частная сеть», суть которой сводится к тому, что сетевое соединение осуществляется посредством стороннего подключения. Иными словами, домашняя сеть используется именно для возможности подключения к иной (сторонней) сети, от имени которой осуществляется регистрация пользователя при реализации доступа к данным. В настоящее время VPN-сервисы очень часто задействуются для обхода блокировок, введенных Роскомнадзором, и продолжения успешного использования запрещенных ресурсов на территории России [5, стр. 32], однако суть их использования заключается в том, чтобы скрыть свой истинный информационный след и «заменить» его подложным, что достигается благодаря применению средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств защиты от повторов и изменений передаваемых по логической сети сообщений). Также виртуальные частные сети (VPN) и другие инструменты для маскировки и сокрытия IP-адресов и их онлайн-активности используют преступники для онлайн-продаж наркотиков [6, стр. 175].

Схематично алгоритм приведен на рисунке 1:

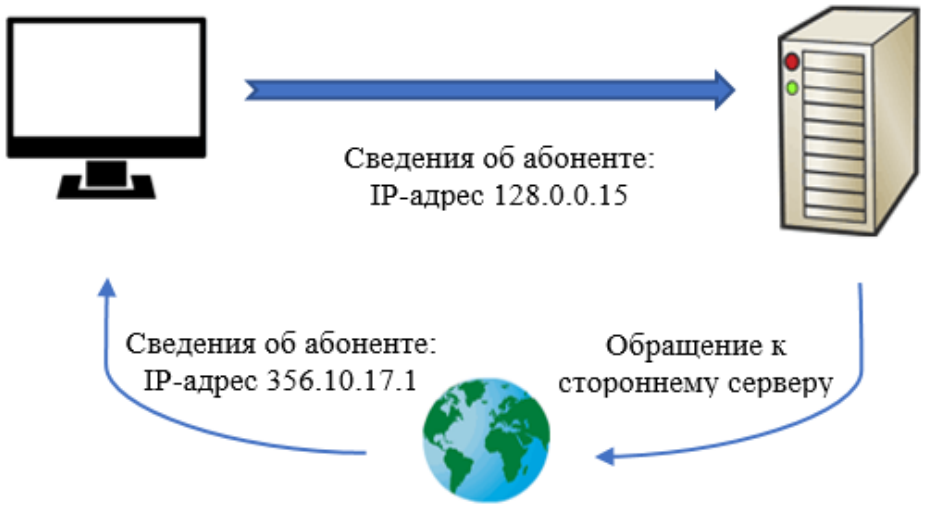

Рис. 1. Схема работы VPN-сервисов

Анонимизация в информационной среде является основой для реализации противоправной деятельности. Преступники избирают определенный способ совершения преступления, включающий в себя подготовку, совершение и сокрытие следов преступления, которые, в свою очередь, должны быть максимально «незаметными» в виртуальной среде. Именно для минимизации оставленных в цифровом пространстве следов изначально разрабатывался и создавался «Даркнет». Учитывая, что цифровые следы в настоящее время подвергаются активному изучению, разрабатываются методики их обнаружения и изъятия, возможности «теневого интернета» становятся все более и более востребованными со стороны лиц криминальной направленности для осуществления противоправной деятельности.

Кратко рассмотрим алгоритм работы в «Даркнете» для возможности понимания его общей концепции. Итак, «Тёмный интернет» позволяет поддерживать высокую степень анонимности. При работе в «обычном» интернете любой запрос, обращение к информации, переадресация с сервера на сервер и т. д. оставляет следы в виде регистрации этого обращения. В отличие от общераспространенного интернета, «Даркнет» начинает свою анонимность еще с момента обращения к нему. Невозможно им пользоваться, обладая познаниями только лишь общего характера, необходимо знать, что доступ в анонимный виртуальный мир становится доступным с использованием специального программного обеспечения. Так, использовать общераспространенные браузеры-программы для поиска и просмотра информации из сети интернет, для доступа в «Даркнет» не получится по техническим причинам. Для этих целей существуют специализированные «проводники» – браузеры, обладающие определенным специфическим встроенным функционалом, к которым относятся такие как Tor, I2P, GNU IceCat и другие. Именно при помощи указанного программного обеспечения осуществляется маршрутизация запроса пользователя, который проходит множественное преобразование путем шифрования, благодаря чему весьма затруднительной становится возможность дешифрования запроса и получение сведений об его отправителе. Использование подобного рода программ, которые зачастую являются легальными, свидетельствует о

технической осведомленности пользователя относительно «правил» доступа к информации с соблюдением особенных правил конфиденциальности, о наличии у него навыков работы с электронно-вычислительными машинами, что в свою очередь подтверждает факт того, что познание личности преступника осуществляется через «процесс познания признаков, свойств и состояний лица» [7, с. 15].

Так, обращаясь к алгоритму обмена данными в «Темном интернете», О. А. Дворянкин достаточно доступно описывает алгоритм работы «Даркнета», который заключается в том, что при подключении пользователя к сайтам через несколько узлов по всему миру, используя информационный ресурс в одном государстве, браузер может перенаправить его через иную страну, а зачастую и не одну, в том числе и на разных континентах, что позволяет пользователям «Даркнета» получать практически полную анонимность при использовании своих ресурсов [8, с. 16].

Следует понимать, что случайно попасть на электронный ресурс в «Даркнете» практически невозможно. Кроме специализированного программного обеспечения, пользователю необходимо знать конкретный адрес информационного ресурса. Так, для «Даркнета» характерным является то, что адреса сайтов заканчиваются указанием доменов «.onion», что является своего рода маркером того, что подобные сайты могут быть противоправноориентированными. При этом само имя сайта (без указания домена – обозначение до точки) в большинстве случаев содержит в названии набор разнообразных (случайных) 16-значных символов, которые никак не проявляют противоправной направленности ресурса (например, 5jfpHK332MnBN27.onion).

«Даркнет», как информационный ресурс, предоставляет пользователям не только возможность конфиденциального общения и обмена информацией, но и возможность анонимного приобретения товаров и услуг, которые зачастую носят характер противоправных. Следует отметить, что приобретаться могут не только материальные объекты (наркотические средства, фальшивые денежные средства, огнестрельное оружие, холодное оружие, похищенное имущество, сфальсифицированные документы и т. д.), но и информация – информационные сведения (документы ограниченного доступа, базы данных, персональные денные, сведения из финансово-кредитных организаций и т. п.).

При этом отметим, что для максимальной степени анонимности в «Даркнете» не принято использовать общепринятые способы оплаты (наличный расчет, безналичные переводы, бартер, взаимозачеты и т. д.), а распространение получило осуществление расчетов в криптовалюте, которая изначально задумывалась как платежная единица, создаваемая «для обеспечения в системе виртуальных платежей децентрализованного характера» [9, с. 43]. Первые упоминания о криптовалюте датируются 1983 годом, однако до 2008 года повсеместного распространения она не имела, пока человек или группа лиц под псевдонимом Сатоши Накамото (Satoshi Nakamoto) не создали всем известный «БитКоин» («BitCoin»), который первостепенно ассоциируется при упоминании криптовалют. Однако это не единственный ее вид, иные криптовалюты также весьма распространены (DogeCoin – DOGE, USDC, Ethereum – ETH, Tether – USDT и многие другие). Тем не менее все криптовалюты сводятся к тому, что они обладают определенными свойствами, такими как:

1. ***Стоимостью.*** Каждая единица криптовалюты имеет свой курс, который, как и в случае с любой общепризнанной валютой, может варьироваться в меньшую или большую сторону в зависимости от разнообразных факторов.

2. ***Анонимностью.*** Любая информация о держателе криптовалюты не только не может быть получена свободным образом, данная информация в принципе никак не коррелирует с данным лицом, отсутствует такая возможность в принципе.

3. ***Рентабельностью.*** Это относительный показатель экономической эффективности. То есть криптовалюта практически всегда востребована, так как позволяет человеку хранить финансовый объем в такой валюте, хоть и виртуальной, которая позволяет иметь значительно большие финансовые свободы.

Возможно ли, имея представление об общем алгоритме действий «Даркнета» и сопутствующих факторах анонимизации, если не в полном объеме, то хотя бы частично пресекать противоправную деятельность криминальных элементов? Действительно, наличие высокой степени анонимного статуса в виртуальном пространстве позволяет пользователю совершать противоправные действия либо осуществлять подготовку к ним с высокой долей вероятности того, что он не будет выявлен. Однако анонимность в «Даркнете» не является безусловной, существуют способы, которые позволяют установить цифровые следы (IP-адрес пользователя, его диалоги и обращения к определенным ресурсам и т. д.), которые в настоящее время отличаются разной степенью эффективности. Рассмотрим некоторые из них, которые в свою очередь будут представляться как информационные атаки на противоправные коммуникации.

- Не всегда браузер и канал связи в силу технических возможностей могут создать выделенный канал коммуникации между специальным сервером злоумышленника, который может регистрировать реальный IP-адрес клиента. По этой причине появилась возможность при помощи специального программного обеспечения устанавливать истинные IP-адреса пользователей. Однако разработчики браузеров оперативно отреагировали на данную проблему и исправили соответствующие ошибки в программном коде. Именно поэтому данный способ в настоящее время устарел и не является актуальным.
- Иным, более современным способом установления индивидуализирующих данных пользователя «Даркнета» является использование специальной библиотеки WebRTC (технология, предназначенная для организации передачи потоковых данных), которая предназначена для организации канала передачи видеопотока между браузерами с поддержкой HTML5 (язык разметки, включающий в себя атрибуты и функционал сайтов и Web-приложений), и дает возможность установить реальный IP-адрес. Направляемые STUN-запросы (сетевой протокол, позволяющий узнавать внешние IP-адреса) от WebRTC поступают в незашифрованном виде в обход браузера, в связи с чем представляется возможным установление индивидуализирующих признаков пользователя. Однако и данный «промах» в программном коде браузеров оперативным образом был устранен, что опять же привело к минимизации деанонимизации пользователя.

Оперативное выявление слабых мест «Даркнета» не менее оперативным образом вызывает их «исправление», именно по этой причине активная работа по поиску-исправлению уязвимых мест являет-

ся актуальной практически постоянно. В настоящее время ведется разработка и проверка на практике и иных способов получения доступа к информации о пользователе «Даркнета», которые неразрывно связаны с необходимостью применения специальных знаний в области цифровых технологий. Однако следует понимать, что на всякое действие, направленное на устранение или минимизацию анонимности, всегда будет иметь место разработка иных способов, направленных на сохранение анонимизации. Р. В. Федоров сказал, что существует круг лиц, которые «хотели бы пользоваться возможностями глобальных сетей и при этом скрывать свой IP-адрес и другие идентификаторы» [10, с. 35], и с ним невозможно не согласиться.

Нередкими являются случаи реализации анонимности самих ресурсов, а не только пользователей. Как правило, подобного рода интерактивные ресурсы содержат в себе запрещенную или ограниченную к свободному доступу информацию, которая может быть размещена в свободном доступе, либо предоставлена за материальное вознаграждение. И если в случае установления данных пользователя возникают сложности с его идентификацией, то для ограничения доступа к указанным информационным ресурсам подобного рода сложностей может возникать значительно меньше в случае своевременного реагирования на их появление. Так, в Российской Федерации с 2012 года ведется законотворческая работа, направленная на реализацию упорядоченной работы в сети интернет. Одним из ее результатов является создание и функционирование Единого реестра доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено[1]. Единый реестр функционирует в соответствии с действующим законодательством. В основе его лежат такие нормативно-правовые акты, как Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ и Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ.

Из изложенного следует, что ограничивать доступ к информационным ресурсам, несущим в себе потенциальную угрозу принципам Конституции Российской Федерации, представляется возможным двумя способами:

а) законодательным ограничением – разработкой и принятием нормативно-правовых актов в сфере использования информационных ресурсов, их доступности и возможных ограничений;

б) физической блокировкой (ограничением) – непосредственным запретом доступа к информационным ресурсам путем внесения ограничений в телекоммуникационном оборудовании.

Как показывает складывающаяся правоприменительная практика, эффективным образом осуществляется ограничительная работа именно в совокупности указанных способов, что позволяет оперативным образом реагировать на вновь появляющиеся угрозы информационного характера, а также угрозы распространения той или иной опасной для общества информации. Именно поэтому выходящие за рамки действующего законодательства информационные ресурсы оперативным образом блокиру-

[1] Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. Официальный сайт [Электронный ресурс]. – URL: https://eais.rkn.gov.ru/ (дата обращения 19.05.2025)

ются, тем самым наглядно демонстрируется корреляция законодательной и физической блокировки.

Выводы и заключение

Подводя итог, следует отметить, что в настоящее время достаточно широкое распространение получили преступления, совершаемые с использованием информационно-телекоммуникационных технологий, однако компетенции, которыми должен обладать субъект расследования подобных преступлений, выходят далеко за рамки юриспруденции и охватывают техническую сторону противоправных действий. Без знания основ кибербезопасности, алгоритмов шифрования и анонимизации, принципов маршрутизации и фиксации интерактивных следов, процесс расследования указанных преступлений в значительной степени замедлится, а эффективность ощутимо снизится. Именно поэтому к расследованию должны привлекаться такие субъекты расследования, которые представляют себе принципы обмена данными и их особенности в информационно-телекоммуникационных технологиях, либо же специалисты в данной сфере на протяжении всего процесса расследования.

СПИСОК ИСТОЧНИКОВ

1. *Грибунов, О. П., Пермяков, А. Л.* Способы совершения хищений, связанных с осуществлением инвестиционных проектов на предприятиях железнодорожного транспорта // Известия Иркутской государственной экономической академии. 2015. Т. 25. № 6. С. 1098–1107.

2. *Старичков, М. В., Лантух, Н. В.* О предмете компьютерной криминалистики // Криминалистика: вчера, сегодня, завтра. 2023. № 3 (27). С. 198–205.

3. *Рудых, А. А.* Криптография и криминалистика: современные проблемы и возможные пути решения // Вестник Восточно-Сибирского института МВД России. 2019. № 2(89). С. 203–212.

4. *Степаненко, Д. А.* Технология собирания электронно-цифровых доказательств: проблемы и рекомендации // ГлаголЪ правосудия. 2024. № 1(35). С. 23–29.

5. *Винокуров, М. В.* Особенности квалификации незаконного оборота медицинской продукции, совершаемого с использованием средств массовой информации или информационно-телекоммуникационных сетей, в том числе сети «Интернет» // Криминалистика: вчера, сегодня, завтра. 2024. № 3(31). С. 30–37.

6. *Усачев, С. И.*, *Завьялов, А. Н.* Особенности раскрытия, расследования и предупреждения преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ в условиях цифровизации // Юристъ-Правоведъ. 2023. № 1(104). С. 172–177.

7. *Ганиева, И. А*. Личность преступника, совершающего дистанционное мошенничество // Актуальные вопросы борьбы с преступлениями. 2023. № 5. С. 15–18.

8. Дворянкин, О. А. Даркнет - темная сторона Интернета или неужели так все плохо // Национальная Ассоциация Ученых. 2021. № 71-1. С. 14–20.

9. *Дворянкин, О. А.* Информационные технологии, противодействующие распространению преступлений, совершаемых в сети интернет с применением криптовалюты // Тенденции развития науки и образования. 2022. № 86-7. С. 41–45.

10. *Федоров, Р. В.* Теоретико-правовые аспекты права на анонимность в сети Интернет // Юридический вестник Дагестанского государственного университета. 2022. Т. 44. № 4. С. 34–41.

REFERENCES

1. *Gribunov, O. P., Permyakov, A. L.* Sposoby sovershеniya khishcheniy, svyazannykh s osushchestvleniyem investitsionnykh proyektov na predpriyatiyakh zheleznodorozhnogo transporta [Methods of embezzlement associated with the implementation of investment projects at railway transport enterprises]. Izvestiya Irkutskoy gosudarstvennoy ekonomicheskoy akademii – Izvestia of the Irkutsk State Economic Academy. 2015, vol. 25, no. 6, pp. 1098–1107. (in Russian).

2. *Starichkov, M. V., Lantukh, N. V.* O predmete komp'yuternoy kriminalistiki [On the subject of computer forensics]. Kriminalistika: vchera, segodnya, zavtra – Forensics: yesterday, today, tomorrow. 2023, no. 3(27), pp. 198–205. (in Russian).

3. *Rudykh, A. A.* Kcryptografiya i kriminalistica: sovremennye problemy i vozmozhnye puti resheniya [Cryptography and criminalistics: modern problems and possible ways of solution]. Vestnik Vostochno-Sibirskogo instituta MVD Rossii – Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2019, no. 2(89), pp. 203–212. (in Russian).

4. *Stepanenko, D. A.* Tekhnologiya sobraniia elektronno-tsifrovykh dokazaniy: problemy i rekomendatsii [Technology of collecting electronic-digital evidence: problems and recommendations]. Glagol" pravosudiya – Verb of justice. 2024, no. 1(35), pp. 23–29. (in Russian).

5. *Vinokurov, M. V.* Osobennosti kvalifikatsii nezakonnogo oborota meditsinskogo produktiv, sovershaemnogo s ispol'zovaniye sredstva massi informatsii ili informatsionno-telekommunikatsionnykh seti, vincluding seti "Internet" [Features of the qualification of illegal circulation of medical products, committed with the use of mass media or information and telecommunication networks, including the Internet network]. Kriminalistika: vchera, segodnya, zavtra – Forensics: yesterday, today, tomorrow. 2024, no. 3(31), pp. 30–37. (in Russian).

6. *Usachev, S. I., Zavyalov, A. N.* Osobennosti raskrytiza, rassledovanie i preduprezhdeniya prestupleniya, svyazannykh s nezakonnom oborotom narkoticheskikh sredstva i psikhotropnykh veshchestva v usloviyakh tsifrovatsii [Features of disclosure, investigation and prevention of crimes related to illegal trafficking of narcotic drugs and psychotropic substances in the conditions of digitalization]. Yurist-Pravoved – Jurist-Pravoveda 2023, no. 1(104), pp. 172–177. (in Russian).

7. *Ganieva, I. A.* Lichnost' prestupnika, sosovershayuschego distantsionnoe swindlem [Personality of a criminal who commits a remote fraud]. Aktual'nyye voprosy bor'by s prestupleniyami – Topical Issues of Combating Crime. 2023, no. 5, pp. 15–18. (in Russian).

8. *Dvoryankin, O. A.* Darknet - temnaya storona Interneta ili neuzheli tak vse plokho? [Darknet - the dark side of the Internet or really everything is bad]. Natsional'naya Assotsiatsiya Uchenykh – National Association of Scientists. 2021, no. 71-1, pp. 14–20. (in Russian).

9. Dvoryankin, O. A. Tendentsii razvitiya nauki i obrazovaniya [Trends in the development of science and education]. Tendentsii razvitiya nauki i obrazovaniya – Trends in science and education 2022, no. 86-7, pp. 41–45. (in Russian).

10. Fedorov, R. V. Teoretiko-pravovye aspekty prava na anonimnost' v seti Internet [Theoretical and legal aspects of the right to anonymity on the Internet] Yuridicheskiy vestnik Dagestanskogo gosudarstvennogo universiteta – Legal Bulletin of Dagestan State University. 2022, vol. 44, no. 4, pp. 34–41. (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Милюс Александр Иозосович, кандидат юридических наук, заместитель начальника кафедры криминалистики. Восточно-Сибирский институт МВД России. 664074, Российская Федерация, г. Иркутск, ул. Лермонтова, 110.

INFORMATION ABOUT THE AUTHOR

Alexander I. Milius, Candidate of Legal Sciences, Deputy Head of the Forensic Science Department. East Siberian Institute of the MIA of Russia. 110, Lermontov st., Irkutsk, Russian Federation, 664074.