Научная статья

УДК 343.98
DOI 10.25205/2542-0410-2024-20-4-50-59

Даркнет в системе обеспечения безопасности киберпространства

Александр Борисович Смушкин

Саратовская государственная юридическая академия
Саратов, Россия

Skif32@yandex.ru, https://orcid.org/0000-0003-1619-8325

Аннотация

Автором констатируется активное использование теневого интернета преступной средой при явном отставании криминалистических исследований данного сегмента сети Интернет. Автор рассматривает основы функционирования сети Даркнет и утверждает, что повышенный уровень анонимизации данной сети обусловлен одноранговым взаимодействием, луковичной и туннельной маршрутизацией, каскадами перемешивания, многоступенчатой передачей данных и иными методами. В статье указывается, что основные криминалистические методы работы с даркнетом направлены на взлом, извлечение и исследование информации из некоторых сервисов даркнета, деанонимизацию и идентификацию пользователей. Автором предлагаются рекомендации, связанные с использованием при работе в сети Даркнет пиринговых сетей и на луковичной маршрутизации. Подчеркиваются перспективы использования нейросетей, предназначенных для анализа больших данных (Big Date).

Ключевые слова

криминалистическое исследование, даркнет, пиринговые сети, туннельная маршрутизация, TheOnionRouter, деанонимизация пользователя, незаконный контент

Финансирование

Исследование выполнено за счет гранта Российского научного фонда по проекту «Кибербезопасность: уголовно-правовые, криминологические и криминалистические аспекты» № 24-28-00312, https://rscf.ru/project/24-28-00312/

Для цитирования

Смушкин А. Б. Даркнет в системе обеспечения безопасности киберпространства // Юридическая наука и практика. 2024. Т. 20, № 4. С. 50–59. DOI 10.25205/2542-0410-2024-20-4-50-59

Darknet in the Cyberspace Security System

Alexander B. Smushkin

Saratov State Law Academy, Saratov,
Russian Federation

Skif32@yandex.ru, https://orcid.org/0000-0003-1619-8325

Abstract

The author states the active use of the Shadow Internet by the criminal environment with a clear lag in forensic research of this level of the Internet. It should be borne in mind that although the Shadow Internet contains, according to various data, from 0.1 to 1% of the information of the entire Internet, but its active use for criminal purposes requires scientific study. The author examines the basics of the functioning of the Darknet network and states that the increased level of anonymization of this network is due to peer-to-peer interaction, onion and tunnel routing, mixing cascades, multi-stage data transfer and other methods. The article indicates that the main criminalistic methods of working with Darknet are aimed at hacking, extracting and researching information from some Darknet services, de-anonymizing and identifying users. The use of neural networks designed for Big Data analysis (Big Date) can be of great benefit in terms of de-an-

onymization of suspects on the Darknet network. The author offers recommendations related to the use of peer—to-peer networks based on tunnel routing technologies 2IP (Invisible Internet Project – invisible Internet) and The Onion Router when working on the Darknet network. Summing up, the author states that the fight against illegal content and the use of the Shadow Internet for criminal purposes should be conducted comprehensively and systematically

Keywords

forensic investigation of the Darknet, peer-to-peer networks, tunnel routing, TheOnionRouter, deanonymization of the user, illegal content

Funding

The research was funded by the grant of the Russian Science Foundation under the project “Cyber security: criminal-legal, criminological and criminalistic aspects”, № 24-28-00312, https://rscf.ru/project/24-28-00312/

For citation

Smushkin A. B. Darknet in the cyberspace security system. *Juridical Science and Practice*. 2024, vol. 20, no. 4, pp. 50–59. (in Russ.) DOI 10.25205/2542-0410-2024-20-4-50-59

Современные преступники активно эксплуатируют криминогенный потенциал анонимизации теневого интернета. Научное же сообщество, к сожалению, только начало уделять внимание криминалистическому исследованию данной части сети Интернет и по сравнению с исследованием тех же социальных сетей или электронных доказательств содержит в разы меньше публикаций. Что же собой представляет данный уровень сети Интернет? По данным Р. А. Исканова и Г. С. Слепова, термин «даркнет» впервые был упомянут в книге сотрудников компании Майкрософт, посвященной вопросам обеспечения конфиденциальности в сети Интернет» [1, с. 271–273]. Даркнет, в основном, построен на одноранговом взаимодействии. Да и при использовании браузера TOR существенно отличается иерархия сети от классической архитектуры «клиент – сервер» за счет появления множества промежуточных НОДов.

При этом теневой интернет содержит только порядка от 0,1 до 1 % информации всего интернета [2, с. 651]. Преступность в сфере даркнета может быть связана: с контентом сексуального характера; незаконной торговлей запрещенными к обороту объектами (оружием, наркотиками, поддельными документами), экономической преступностью, преступностью в сфере компьютерной информации; экстремистской преступностью, насильственной преступностью, преступностью в сфере интеллектуальной собственности и «пиратства». Отдельно можно сказать о реализуемых на площадках даркнета предложениях «Преступление как услуга» – заказ поджогов, насильственных преступлений, терактов и диверсий, а также «Вредоносное ПО как услуга» – возможность приобретения вредоносного кода, а также инфраструктуры для его распространения.

В. Б. Вехов выделяет следующие технологии, используемые в даркнете:

1) специальные поисковые системы (интернет-браузеры);

2) технологии, предназначенные для обмена информацией между пользователями. Это так называемые «файлообменники» и «мессенджеры»;

3) анонимайзеры;

4) операционные системы специального назначения [3, с. 266–271].

Однако перечисленными способы сокрытия и анонимизации при использовании теневого интернета не исчерпываются. Злоумышленник может использовать VPN-сервера, которые «обрубают» информацию, индивидуализирующую пользователя, и все его запросы, фактически отправляют от своего имени, proxy-серверы, позволяющие скрыть IP-адрес пользователя, динамический IP-адрес. Да и просто могут выходить в сеть только из интернет-кафе, используя для регистрации одноразовые почтовые ящики или специальное программное обеспечение.

При применении TOR используется многослойное шифрование и многоступенчатая передача данных. Как указывают Ю. А. Бондаренко и Г. М. Кизилов, «маршрутизатор вначале передачи информации выбирает случайное число промежуточных маршрутизаторов и генерирует CREATE-сообщения, шифруя их симметричным ключом и указывая для каждого маршрутиза-

тора, какой маршрутизатор будет следующим на пути» [4, с. 99]. Таким образом, сеть промежуточных НОД и многослойное шифрование не дают установить источник, адресат и точный маршрут прохождения запроса.

Сравнительно небольшое распространение имеет еще один сервис анонимизации в сети Даркнет – JonDonym, в котором используются каскады перемешивания (используется несколько последовательных серверов перемешивания, на которых трафик каждого пользователя смешивается с трафиком других участников).

Все вышеуказанное существенно осложняет привлечение к ответственности лиц, подготавливающих или совершающих преступление с использованием данного сегмента сети Интернет.

Рассмотрим криминалистические аспекты исследования даркнета и противодействия преступности в теневом интернете.

В первую очередь, необходимо отметить применение специфической криминалистической техники – аппаратно-программных комплексов, технологий и методов цифровой криминалистики.

Расследование любого преступления, сопряженного хотя бы частично с использованием даркнета, связано с обязательным использованием соответствующих программных инструментов, имеющих функционал, направленный на взлом, извлечение и исследование информации из некоторых сервисов даркнета, деанонимизацию и идентификацию пользователей, установление их географического местонахождения на момент действий в киберпространстве даркнета.

Учеными разных стран предлагаются разные пути борьбы с преступными проявлениями использования теневого интернета, однако полностью решающих все проблемные вопросы методов цифровой криминалистики до сих пор не предложено.

Ряд исследователей предлагают использование математического аппарата сетевого профайлинга в криминалистических целях. Эту задачу у них предлагают решить при анализе форумов и социальных сетей в даркнете «путем построения ориентированной коммуникационной сети, лежащей в основе форума, где узлами являются участники, публикующие сообщения, а дугами – ответы на оригинальные сообщения. Это позволяет нам рассчитать характеристики узлов, такие как количество входящих и исходящих дуг (индеградиентность и центральность), а также показатели, относящиеся ко всей сети, такие как плотность и централизация. Плотность – это процент потенциальных связей, наблюдаемых в сети, и она отражает уровень сплоченности сети. Централизация относится к распределению узловой центральности по всей сети и описывает степень, в которой сетевая связность организована вокруг одной или нескольких фокусных точек» [5]. Используя подобные методы анализа, можно построить примерные социальные графы участников криминальных форумов.

Дивья Барония дифференцирует криминалистические методы обнаружения использования даркнета на «обнаружение артефактов в операционной системе, артефактов сетевого трафика, вредоносных плагинов, снятие и анализ дампа памяти и др.» [6]. Однако представляется, что предложенные ей варианты способствуют только подтверждению факта использования TOR и даркнета, что в большинстве стран не преступно, или, как минимум, не наказуемо. Само же содержание деятельности, объем трафика, адреса интернет-серфинга и т. д. останутся скрытыми.

Ю. А. Бондаренко и Г. М. Кизилов, рассматривая методы привлеченных к расследованию преступления специалистов в области компьютерных технологий, разделили действия по взлому и деанонимизации сети TOR на пассивные и активные. «Пассивные: анализ трафика пользователя, основанный на установлении временно́й взаимосвязи между запросом на создание соединения и установкой выходного соединения; другие, основанные на анализе трафика и нагрузки узла внутри сети. Активные действия: комбинированные действия Tagging – дублирование случайного сообщения на входном узле, его поиск в поступивших на выходной

узел данных; Raptor – серия действий по асимметричному анализу трафика, сбору и обработке информации о перебоях, которые приводят в силу специфики топологии и протоколов работы анонимной сети данные на нужный узел, с последующим собиранием проходящего трафика» [4, с. 99].

А. В. Новосельцева и С. Г. Клюев в рамках действий в ходе атак деанонимизации, которые можно использовать в криминалистической деятельности для установления пользователя, указывают, что «активные действия характеризуются изменением сведений, содержащихся в данных, а также отображением совершаемых действий в сети и называют также следующие методы: активные действия состоят в совокупном тайминге https-трафика, направления оповещения отслеживающему серверу и копирования произвольного сообщения на входном узле, его отбор в определившихся на выходной узел данных с целью осложнения сетей и затруднения обмена данных с затягиванием на управляемый канал учета множества пакетов информационных данных» [7, с. 156–157].

Группа американо-итальянских исследователей настаивает на возможности с 80%-й вероятностью «деанонимизации запроса, прошедшего цепочку анонимизации в сети TOR с использованием предоставленных маршрутизаторами через Netflow метаданных о потоках файлов при обращении к подконтрольному ресурсу по всплескам трафика, которые можно сопоставить с некоторыми параметрами передаваемого пакета информации» [8]. Однако обращение злоумышленников к подконтрольному правоохранительным органам и спецслужбам ресурсу навряд ли можно назвать повсеместным. Скорее, это можно реализовать только в ситуациях создания копий торговых площадок (маркетплейсов) или перехвата управления площадками, либо умышленной дезинформации и организации с помощью рефлексивного управления или социальной инженерии, установки именно тех установочных файлов, в которые уже внедрены бэкдоры (от англ. back door – «черный ход», «задняя дверь) – специально предусмотренные уязвимости, обеспечивающие доступ к устройствам или взлом аккаунтов. Теоретически в целях деанонимизации пользователя правоохранительные органы могут также использовать метод, основанный на файле-приманке, открытие которого направляет на сервер IP-адрес злоумышленника (анонимность TOR действует только на сайты, открываемые в нем, но перекачанные на компьютер файлы – уже «забота» пользователя). Однако при этом остается открытой задача стимулирования перекачки конкретного файла и открытия его не в «песочнице» или иной виртуальной машине. Фактически стимулирование установки именно требующегося правоохранительным органам программного обеспечения возможно только с помощью криминалистической тактической операции.

Теоретически в криминалистических целях можно попытаться внедрить в систему подконтрольные узлы. Однако эта мера не гарантирует полностью деанонимизацию злоумышленника, поскольку даже при получении контроля над 30 % узлов определенной НОДы вероятность 2/3, что информация конкретного пользователя пройдет через другие узлы.

Новозеландские ученые указывают что «артефакты, подтверждающие установку и использование браузера TOR, генерируются в памяти и на диске в виде закладок по умолчанию даже после деинсталляции программы, активность же пользователей в сети TOR получает свое отражение в реестре Windows 10» [9]. Исследование подобных артефактов осуществляется в рамках осмотра компьютера специалистами или компьютерно-технической экспертизы экспертами.

Особое внимание следует уделить криминалистическим тактическим рекомендациям и рекомендациям по тактике оперативно-розыскного обеспечения в области противодействия преступлениям с использованием теневого интернета.

Относительно даркнета представляется необходимым отдельно рассматривать криминалистические рекомендации по пиринговым сетям на основе технологий туннельной маршрутизации 2IP (Invisible Internet Project – невидимый интернет) и луковичной маршрутизации The Onion Router.

В случае использования пиринговых одноранговых сетей в криминальных целях представляется, что внешний доступ в них возможен только по приглашению действующего пользователя, что повышает значение оперативно-розыскного потенциала в плане внедрения в число пользователей сети своего сотрудника, вербовки пользователя или иного получения доступа к учетной записи действующего пользователя.

При расследовании преступлений, при совершении которых использовался браузер TOR, особую роль должно играть отслеживание взаимосвязей открытого интернета с даркнетом (указание в одном адресов или иных данных пользователя в другом), проведение следственного осмотра маркетплейса для ознакомления с правилами пользования, а также ассортиментом незаконных предложений конкретных торговцев, проведение проверочных закупок, создание копий торговых площадок или перехват управления площадками, собственники и модераторы которых задержаны, и проведения оперативного эксперимента, контролируемых поставок. Зарубежные криминалисты указывают на то, что «полезно анализировать форумы ClearNet, поскольку они предоставляют информацию о новых пользователях даркнет-маркетов, их мотивации и проблемах» [10].

Многие сайты даркнета требуют приглашений доверенных пользователей. В этом случае повышается важность агентурной работы и вербовки этих пользователей.

Кроме того, в криминалистических целях возможна корреляция транзакций с криптовалютой, отслеживание закупок, идентификация продавца и покупателя с помощью блокчейна и использование других методов.

Среди общих средств можно отметить оперативный мониторинг как открытого интернета, так иных его сегментов, особенно даркнета. О необходимости изменения правого статуса мероприятий по мониторингу сетевых ресурсов и электронных баз данных мы уже говорили в своих предыдущих работах [11, с. 220, 221, 227]. Как отмечают А. А. Белоусов и А. М. Васильев, «основными направлениями мониторинга, способными обеспечить высокую интенсивность поступления оперативно-розыскной информации, являются: а) автоматизированный поиск сетевых информационных ресурсов, содержащих запрещенную к распространению информацию; б) оперативно-розыскное изучение выявленных сетевых ресурсов, связанных с деятельностью преступных сообществ; в) наблюдение за закрытыми для общего доступа местами сетевого общения криминальной направленности. По результатам поиска принимаются меры к блокированию сайтов и установлению личности их организаторов» [12, с. 36]. Оперативно-розыскное обеспечение может осуществляться как при самостоятельной оперативной разработке преступных групп, так и по поручению следователя, при расследовании преступлений.

Оперативно-розыскная разработка и криминалистическое исследование может вестись как в отношении оператора (предполагаемого оператора) криминального маркетплейса в даркнете, так и в отношении пользователей, делающих криминальный заказ. Методы работы здесь будут различаться. Как отметили Daniel Dolejška, Michal Koutenský, Vladimír Veselý, Jan Pluskal, в первом случае «лица, представляющие интерес, <…> находятся под наблюдением, и создается журнал того, что они делают. Журнал также может включать их присутствие в Сети в определенное время (т. е. то, чем они делились в социальных сетях). Такой журнал обеспечивает идеальный источник данных для взаимной корреляции с данными о действиях оператора / сервисных событиях в dark web»; во втором «возможно получение следующей информации о пользователе: а) активность пользователя – регулярная или кажущаяся случайной; б) часовой пояс пользователя (на основе временных меток наблюдаемых событий); и в) совпадение событий и их закономерностей с другими наблюдаемыми действиями, собранными OSINT» [13].

Достаточно часто при дистанционной торговле незаконными объектами через даркнет задерживаются именно получатели заказа. В распоряжении следствия и суда оказываются протоколы допроса задержанного в стиле «20 мая 2020 года примерно в 20 часов 00 минут он находился у себя дома, когда примерно в 20 ч. 10 мин. с помощью своего мобильного телефона

марки «Honor 8 A» через браузер «TOR BROWSER» зашел на сайт «Гидра», где указаны наименования наркотических средств, и выбрал пункт «Марихуана», появились массы на выбор, он нажал кнопку «купить 3 грамма», далее на экране появилась надпись: оплатите на баланс телефона и был указан номер телефона и стоимость. Он оделся и пошел в терминал для оплаты заказа наркотического средства. Через какое-то время на сайте «Гидра» высветились координаты с фотографией места закладки, где были спрятаны наркотические средства»[1]; «имея умысел на незаконное приобретение без цели сбыта наркотических средств в значительном размере, действуя из личной заинтересованности, выраженной в желании потребить наркотическое средство, обладая информацией о возможности приобретения наркотических средств на территории города Петрозаводска у неустановленного лица путем их получения в оборудованном тайнике – «закладке», договорилась с неустановленным лицом посредством отправления сообщений в установленном в ее телефоне «Samsung» приложении «Tor Browser» на интернет-площадке «Hydra» в информационно-телекоммуникационной сети Интернет о приобретении наркотического средства в значительном количестве; оплатила приобретаемое наркотическое средство путем перечисления 1626.00 рублей посредством мобильного приложения «Сбербанк Онлайн» на полученный от неустановленного лица номер телефона и получила от последнего сообщение с информацией о месте нахождения тайника с наркотическим средством»[2]. Как правило, при этом доказательственной базы может хватить только для привлечения к ответственности заказчика, максимум – кладмена (закладчика). Крайне редко можно отследить финансовые транзакции до конкретного продавца. Представляется, что без введения ответственности администраторов и собственников маркетплейса даже попытка блокирования таких ресурсов, расположенных в даркнете или работающих через зашифрованные каналы Telegram, приводит лишь к появлению «зеркальных» адресов и иных способов обхода блокировки. Так, в одном из изученных нами уголовных дел в приговоре прямо отмечалось относительно маркетплейса Hydra: «вход на данный сайт для пользователей интернета, находящихся на территории России, в соответствии с законодательством РФ заблокирован провайдерами, и при попытке воспользоваться его услугами абонент получает сообщение: «Уважаемый абонент, данный ресурс заблокирован по решению органов государственной власти Российской Федерации». Однако с использованием специальных программ для серфинга в Сети, скрывающих реальный IP-адрес, таких как TOR (расположен на интернет-ресурсе https://www.torproject.org/) и VPN, а также прокси и анонимайзеров (http://anonymouse.org/cgi-bin/anon-www.cgi/http://legalrc.biz, http://www.guardster.com/free/), пользователь может осуществить вход на сайт «Hydra». Также в настоящее время возможно обходить блокировку сайтов через сервисы VPN (Virtual Privat Network) – виртуальную частную сеть, абсолютно защищенный канал, который соединяет электронное устройство с выходом в сеть Интернет с любым другим в Мировой сети»[3].

Таким образом, можно отметить, что преступления, совершаемые с использованием сети Интернет носят дистанционный характер. Это приводит к повышенной анонимности злоумышленников и следовой картине, представленной, преимущественно, виртуальными и идеальными следами.

Наиболее велик криминогенный потенциал даркнета вследствие его повышенной анонимизации. Основные модели правового регулирования даркнета выделили Е. А. Брылева и Ф. М. Велиев:

---

[1] Приговор Оренбургского районного суда Оренбургской области от 21 сентября 2020 г. по делу № 1-245/2020// Архив Оренбургского районного суда оренбургской области.

[2] Приговор Петрозаводского городского суда Республики Карелия от 7 сентября 2020 г. по делу № 1-794/2020// Архив Петрозаводского городского суда Республики Карелия.

[3] Приговор Ухтинского городского суда Республики Коми от 28 июля 2020 г. № 1-284/2020 // Архив Ухтинского городского суда Республики Коми.

«– полный запрет на нормативном уровне использования даркнета в силу того, что данный сегмент сети Интернет используется для совершения преступлений и препятствует идентификации личности злоумышленников;

– недопустимость какого-либо государственного вмешательства в функционирование даркнета, так как его существование определяется реализацией идеи о свободном интернете;

– невозможность полного запрета использования даркнета и нейтральность в части оценки, используемой при функционировании даркнет-технологии, обеспечивающей анонимность пользователей. Тем самым данная модель предполагает выработку и реализацию технических и правовых средств реагирования на ту угрозу, которую представляет собой даркнет» [14, с. 75–80].

Борьба с даркнетом может быть или кардинальной, путем полной блокировки, или адресной. В настоящее время доступ к The Onion Router запрещен, и Роскомнадзор блокирует его, однако существуют программные методы обхода блокировки, да и кроме подобного способа входа в даркнет существуют и иные. Поэтому разумным представляется последний вариант модели, выделенной Е. А. Брылевой и Ф. М. Велиевым.

В пресечении преступлений, совершаемых с использованием любого сегмента сети Интернет, особое значение будут иметь оперативно-розыскные мероприятия: опрос, снятие информации с технических каналов связи, проверочная закупка, оперативный эксперимент, получение компьютерной информации. Из следственных действий на начальном этапе расследования приобретают значение осмотр интернет-страницы (в нашей трактовке это один из видов осмотра электронного объекта), допросы потерпевшего, свидетелей, а в случае обнаружения – допрос подозреваемого. Возможно также назначение различных видов компьютерно-технических экспертиз.

В некоторых случаях осмотр стационарного компьютера без подключения к Сети может также предоставить следствию некоторую информацию об интернет-соединениях и действиях в Сети. Так, по уголовному делу № 1-365/2020, рассмотренному Кировским районным судом г. Томска, свидетель ФИО10 показал, что он был приглашен для участия в проведении осмотра системного блока компьютера. Производился смотр информации, имеющейся на носителях информации, установленных в данном системном блоке. На втором условном логическом диске под названием «Черная хреновина» имелась папка «Доки и прочее», в которой обнаружен файл Hydra.txt, в котором имелись идентификационные данные: логин и пароль для интернет-ресурса. С рабочего стола запускался интернет-браузер под ярлыком Start Tor Brawser. При открытии соединений были введены логин и пароль, указанные выше. Далее производился осмотр открытых закладок, в которых отобразились места на местности с указанием точной местности, координаты, различные тексты, в том числе просматривалась история соединений с информацией о проведении закупки наркотического средства. Данная информация переведена на изображениях, сформирована в фототаблицу, которая была приложена к протоколу осмотра[4]. Указанные обстоятельства подчеркивают важность разработки криминалистических тактических рекомендаций по производству осмотра электронного устройства.

Подводя итог, следует отметить, что борьба с незаконным контентом и использованием теневого интернета в преступных целях должна вестись комплексно и системно. Представляется, что большую пользу в плане деанонимизации подозреваемых в сети Даркнет может принести использование в криминалистических целях нейросетей, предназначенных для анализа больших данных (Big Date). В целях анализа больших данных мы рассматриваем здесь выборку и выявление подозреваемого из массы пользователей, одновременно воспользовавшихся функционалом TOR, а также совершивших определенное действие на отслеживаемом ресурсе.

[4] Приговор Кировского районного суда г. Томска от 21 июля 2020 г. по уголовному делу № 1-365/2020 // Архив Кировского районного суда г. Томска.

В последнее время в РФ к обеспечению пресечения незаконного контента интернета присоединяются также добровольные объединения граждан и организации. Например, Лига безопасного интернета, созданная при поддержке МВД России, Минкомсвязи и Комитета Государственной Думы по вопросам семьи, женщин и детей. В качестве основной цели функционирования Лиги декларируется создание безопасного пространства интернета на территории Российской Федерации. Криминалистические же исследования данного уровня сети Интернет должны «дать в руки» следователю действенные технические, тактические, организационные и методические инструменты исследования даркнета и противодействия использованию его при совершении преступлений.

Кроме того, представляется необходимым установить, как минимум, административную ответственность владельцев законных торговых платформ за непроведенную модерацию контента (выявленную продажу товаров, ограниченных в обороте или изъятых из оборота, через определенную торговую площадку).

Список литературы

1. **Иксанов Р. А., Слепов Г. С.** Защита прав граждан от посягательств в сети Даркнет // Международный журнал гуманитарных и естественных наук. 2018. № 4. С. 271–273.
2. **Узденов Р. М.** Новые границы киберпреступности // Всероссийский криминологический журнал. 2016. Т. 10, № 4. С. 649–655.
3. **Вехов В. Б. и др.** Цифровая криминалистика: Учебник для вузов. 2-е изд., перераб. и доп. / Под ред. В. Б. Вехова, С. В. Зуева. М.: Юрайт, 2024. 490 с.
4. **Бондаренко Ю. А., Кизилов Г. М.** Проблемы выявления и использования следов преступлений, оставляемых в сети Darknet // Гуманитарные, социально-экономические и общественные науки. 2019. № 5. С. 97–101.
5. **Arjan Blokland, Anton Daser, Meike de Boer, Colm Gannon, Frederic Gnielka, Salla Huikuri, Rebecca Reichel, Thomas Shäfer, Alexander F. Schmidt, Katarzyna Staciwa, Robert Lehmann.** Why do users continue to contribute to darknet Child Sexual Abuse Material forums? Examining social exchange, social capital, and social learning explanations using digital forensic artifacts // Child Abuse & Neglect. 2024. Vol. 153. P. 106815.
6. **Divya Baronia.** Dark Web And Tor Forensic // Informaticss.com URL: https://informaticss.com/dark-web-and-tor-forensic/ (дата обращения: 25.09.2024).
7. **Новосельцева А. В., Клюев С. Г.** Современные методы атак деанонимизации на сеть TOR // Прикаспийский журнал: управление и высокие технологии. 2020. № 1 (49). С. 155–161.
8. **Sambuddho Chakravarty, Marco V. Barbera, Georgios Portokalidis, Michalis Polychronakis, Angelos D. Keromytis Chakravarty S., Barbera M. V., Portokalidis G., Polychronakis M., Keromytis A. D.** On the Effectiveness of Traffic Analysis against Anonymity Networks Using Flow Records. In: Faloutsos, M., Kuzmanovic, A. (eds) Passive and Active Measurement. PAM 2014. Lecture Notes in Computer Science. 2014. Vol. 8362. Springer, Cham. P. 247–257.
9. **Muir, Matt & Leimich, Petra & Buchanan, William.** A Forensic Audit of the Tor Browser Bundle // Digital Investigation. 2019. Vol. 29. 10.1016/j.diin.2019.03.009. pp. 118–128.
10. **Katsiaryna Bahamazava and Rohan Nanda.** The shift of DarkNet illegal drug trade preferences in cryptocurrency: The question of traceability and deterrence // Forensic Science International: Digital Investigation. 2022. Vol. 40.
11. **Смушкин А. Б.** Концепция дистанционной криминалистики. М.: Юрлитинформ, 2024. 256 с.

12. **Белоусов А. А., Васильев А. М.** Особенности при квалификации преступлений в сфере обезличивания криптовалюты виновными лицами // Тенденции развития науки и образования. 2023. № 96-5. С. 31–39.
13. **Dolejška, Michal Koutenský, Vladimír Veselý, Jan Pluskal.** Busting up Monopoly: Methods for modern darknet marketplace forensics // Forensic Science International: Digital Investigation. 2023. Vol. 46, Suppl. P. 301604.
14. **Брылева Е. А., Велиев Ф. М.** Права человека и интернет-пространство: новые реалии // Юридическая наука: история и современность. 2018. № 11. С. 75–80.

References

1. **Iksanov R. A., Slepov G. S.** Protection of citizens' rights from encroachments on the Darknet network. *Mezhdunarodnyi zhurnal gumanitarnykh i estestvennykh nauk*, 2018, no. 4. pp. 271–273 (in Russ).
2. **Uzdenov R. M.** New frontiers of cybercrime. *Vserossiiskii kriminologicheskii zhurnal*, 2016, vol. 10. no. 4. pp. 649–655. (in Russ).
3. **Vekhov V. B. (eds.)** Digital criminalistics: textbook for universitie. 2-ed. Moscow, Yurait publ., 2024, 490 p. (in Russ).
4. **Bondarenko Yu. A., Kizilov G. M.** (2019) Problems of identifying and using traces of crimes left on the Darknet network. *Gumanitarnye, sotsial'no-ekonomicheskie i obshchestvennye nauki*, 2019, no. 5. pp. 97–101. (in Russ)
5. **Arjan Blokland, Anton Daser, Meike de Boer, Colm Gannon, Frederic Gnielka, Salla Huikuri, Rebecca Reichel, Thomas Shäfer, Alexander F. Schmidt, Katarzyna Staciwa, Robert Lehmann.** Why do users continue to contribute to darknet Child Sexual Abuse Material forums? Examining social exchange, social capital, and social learning explanations using digital forensic artifacts. *Child Abuse & Neglect*, 2024, vol. 153, 106815.
6. **Divya Baronia.** Dark Web And Tor Forensic. *Informaticss.com* available at: https://informaticss.com/dark-web-and-tor-forensic/ (accessed: 25.04.2024).
7. **Novosel'tseva A. V., Klyuev S. G.** Modern methods of deanonymization attacks on the TOR network. *Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii*, 2020, no. 1 (49), pp. 155–161.
8. **Sambuddho Chakravarty, Marco V. Barbera, Georgios Portokalidis, Michalis Polychronakis, Angelos D. Keromytis Chakravarty, S., Barbera, M. V., Portokalidis, G., Polychronakis, M., Keromytis, A. D.** On the Effectiveness of Traffic Analysis against Anonymity Networks Using Flow Records. In: Faloutsos M., Kuzmanovic A. (eds) Passive and Active Measurement. PAM 2014. *Lecture Notes in Computer Science*, 2014, vol. 8362. Springer, Cham. pp. 247–257.
9. **Muir, Matt & Leimich, Petra & Bucha***nan, William. A Forensic Audit of the Tor Browser Bundle.* Digital Investigation, 2019, vol. 29. 10.1016/j.diin.2019.03.009. pp. 118–128;
10. **Katsiaryna Bahamazava and Rohan Nanda.** The shift of DarkNet illegal drug trade preferences in cryptocurrency: The question of traceability and deterrence. *Forensic Science International: Digital Investigation*, 2022, vol. 40, 301377.
11. **Smushkin A. B.** The concept of remote criminalistics Moscow, Yurlitinform, 256 p. (in Russ.).
12. **Belousov A. A., Vasil'ev A. M.** Features in the qualification of crimes in the field of depersonalization of cryptocurrencies by guilty persons. *Tendentsii razvitiya nauki i obrazovaniya*, 2023, no. 96-5, pp. 31–39 (in Russ.).
13. **Dolejška, Michal Koutenský, Vladimír Veselý, Jan Pluskal.** Busting up Monopoly: Methods for modern darknet marketplace forensics. *Forensic Science International: Digital Investigation*, 2023, vol. 46, suppl., 301604.
14. **Bryleva E. A., Veliev F. M.** (2018) Human rights and the Internet space: new realities. *Yuridicheskaya nauka: istoriya i sovremennost'*, 2018, no. 11, pp. 75–80 (in Russ.).

Информация об авторе

Смушкин Александр Борисович, кандидат юридических наук, ведущий научный сотрудник к/н проектного офиса научных программ и исследований, доцент кафедры криминалистики Саратовской государственной юридической академии
Researcher ID: AAM-2853-2020
Scopus ID 57202012484

Information about the Author

Alexander B. Smushkin, Candidate of Law, Leading Researcher C/S of the Project Office of Scientific Programs and Research, Associate Professor of the Department of Criminology of the Saratov State Law Academy
Researcher ID: AAM-2853-2020
Scopus ID: 57202012484

Статья поступила в редакцию 04.10.2024;
одобрена после рецензирования 17.10.2024; принята к публикации 25.10.2024

The article was submitted 04.10.2024;
approved after reviewing 17.10.2024; accepted for publication 25.10.2024