Научная статья
УДК 343.98
DOI: 10.17150/2411-6122.2021.4.77-86

О необходимости формирования единой дефиниции «даркнет» в криминалистике

А.А. Протасевич[1]✉, Ю.Б. Скрябикова[2]
[1, 2] Байкальский государственный университет, г. Иркутск, Российская Федерация
[1] ProtasevichAA@bgu.ru✉
[2] trufanovayulia1994@gmail.com

Аннотация. Статья посвящена проблемам борьбы с преступлениями, совершенными с использованием информационно-телекоммуникационных технологий, в частности, с использованием сети Интернет. Криминальные элементы активно используют пространство сети Интернет для ведения бизнеса преступного характера, укрываясь при этом в теневой части сети — Даркнете. Указанная сеть предоставляет злоумышленникам все возможности для укрытия, предоставляя анонимные сети, гарантирующие высокий уровень конфиденциальности. Данный факт существенно осложняет реализацию правоохранительными органами функции по борьбе с преступлениями, совершенными с использованием информационных технологии. Кроме того, проведенный анализ состояния преступности в Российской Федерации показал, что правоохранительная деятельность на сегодняшний день неэффективна в борьбе с преступлениями рассматриваемой категории. Ввиду чего, видится необходимость повышения «цифровой» грамотности сотрудников правоохранительных органов, а также разработка криминалистической базы с учетом цифрового прогресса. В статье предложена дефиниция «Даркнет», раскрывающая сущность данной сети, которая станет отправной точкой в исследовании явления Даркнет, как объекта криминалистики. Проведенное исследование позволит получить новые источники для построения элементов криминалистической характеристики преступлений и частной криминалистической теории расследования преступлений, совершенных с использованием сети Даркнет.

Ключевые слова: Даркнет, информационно-телекоммуникационные технологии, частная криминалистическая теория, преступления, совершенные в сети Интернет, правоохранительные органы.

Для цитирования: Протасевич А.А. О необходимости формирования единой дефиниции «даркнет» в криминалистике / А.А. Протасевич, Ю.Б. Скрябикова. — DOI: 10.17150/2411-6122.2021.4.77-86 // Сибирские уголовно-процессуальные и криминалистические чтения. — 2021. — № 4. — С. 77–86.

Original article

On the Necessity of Developing a Unified Definition of «Darknet» in Criminalistics

A.A. Protasyevich[1]✉, Yu.B. Srkyabikova[2]
[1, 2] Baikal State University, Irkutsk, the Russian Fedaration
[1] ProtasevichAA@bgu.ru✉
[2] trufanovayulia1994@gmail.com

Abstract. The article is devoted to counteracting crimes committed with the use of information-telecommunication technologies, specifically, the Internet. Criminals use the Internet actively to conduct criminal business transactions while

hiding in the shadow part of the net — Darknet. This net provides offenders with opportunities for hiding by offering anonymous nets that guarantee a high level of confidentiality. This fact makes it considerably harder for law enforcement bodies to counteract crimes committed with the use of information technologies. Besides, an analysis of the criminal situation in the Russian Federation showed that law enforcement work of counteracting this type of crimes is not effective at the present stage. Due to this, there is a need for improving the level of "digital" literacy of law enforcement employees as well as the development of a criminalistic base that takes into account the digital progress. The authors offer a definition of "Darknet" that describes the essence of this net and that will become the starting point for researching the Darknet phenomenon as an object of criminalistics. The conducted research will make it possible to obtain new sources for building the elements of criminalistic description of crimes and a special criminalistic theory of investigating crimes committed with the use of Darknet.

Keywords: Darknet, information-telecommunication technologies, special criminalistic theory, cybercrimes, law enforcement bodies.

For citation: Protasyevich A.A., Srkyabikova Yu.B. On the Necessity of Developing a Unified Definition of «Darknet» in Criminalistics. *Sibirskie Ugolovno-Processual'nye i Kriminalisticheskie Chteniya = Siberian Criminal Procedure and Criminalistic Readings,* 2021, no. 4, pp.77–86. (In Russian). DOI: 10.17150/2411-6122.2021.4.77-86.

Сегодня процесс цифровизации охватывает все сферы жизни и деятельности человека, существенно облегчая и упрощая их. Безусловно, нельзя недооценивать вклад цифровых технологий и в борьбу с преступностью, а также предоставление огромного спектра возможностей по их применению в деятельности правоохранителей. Однако, технологии и информационный прогресс приносят правоохранительным органам ровно столько же инновационных методов борьбы с преступностью, как и правонарушителям возможностей уклонения от ответственности [1, с. 204].

Пожалуй, самым негативным последствием цифровизации является то, что наиболее опасные криминальные элементы, такие как, педофилы, наркосбытчики и наркопризводители, экстремисты и террористы, применяют цифровые технологии в целях совершения преступлений, а также укрытия от ответственности. В.Н. Куфлева говорит о становлении «диджитализации» преступности, как о новом криминальном феномене, под которым понимает переход преступной деятельности в интернет-среду для расширения направлений преступной деятельности [2, с. 81].

Виртуальное пространство, в которое сегодня перебазировалась существенная часть преступных элементов, предоставляет злоумышленникам больше возможностей, нежели правоохранителям. Злоумышленники нашли для себя убежище в глобальной сети Интернет, в частности, в его теневой части, так называемой DarkNet. В пространстве Даркнета для преступников есть все возможности для обезличенного ведения бизнеса преступного характера, в виде предоставления анонимных сетей, которые гарантируют высокий уровень конфиденциальности, что существенно осложняет решение первостепенной задачи правоохранителей, а именно, установление лица, совершившего либо причастного к совершению преступления. В данном случае, при реализации функции по борьбе с преступностью в условиях цифровизации, правоохранителям необходимо качественное криминалистическое обеспечение, в виде

разработанных частных криминалистических методик расследования отдельных видов преступлений, совершенных с использованием информационно-телекоммуникационных технологий, а также существует острая необходимость в повышении «цифровой грамотности» сотрудников правоохранительных органов, что требует от сотрудников наличия знаний из разных областей наук, в том числе компьютерных технологий. Заметим, что угроза теневого Интернета уже отмечалась некоторыми авторами работ в этой области [3, с. 112; 4, с. 158]. Авторы отмечают, наибольшую опасность представляет возможность осуществления продажи таких запрещенных предметов, как оружие и наркотики, а также распространение запрещенного контента порнографического, экстремистского содержания. Однако, наиболее популярной противозаконной деятельностью является оборот наркотиков. Кроме того, указанными авторами абсолютно верно отмечается, что правоохранительным органам необходимо не отставать от преступной деятельности, которая стремительно идет вслед за цифровым прогрессом, и совершенствовать свою деятельность по борьбе с преступностью данного рода, используя инновационные методы. Данную позицию авторов, мы полностью разделяем и поддерживаем. В этой связи, нами проводится исследование криминального, равно и криминалистического феномена — Даркнет. Данное исследование, в последующем, послужит нам фундаментом для построения криминалистической характеристики преступлений, совершенных с использованием новых технологий — посредством теневого Интернета (Даркнет), что, в свою очередь, будет являться обязательным элементом в построении частной криминалистической методики расследования преступлений, данной категории.

Проведенный нами анализ состояния преступности в России[1], за период с 2017 г. по июль 2021 г., см. рис. 1 и 2, показал, что преступления, совершен-

[1] Министерство внутренних дел Российской Федерации: офиц. сайт. М., 2021. URL: http://мвд.рф/reports (дата обращения: 29.09.2021).

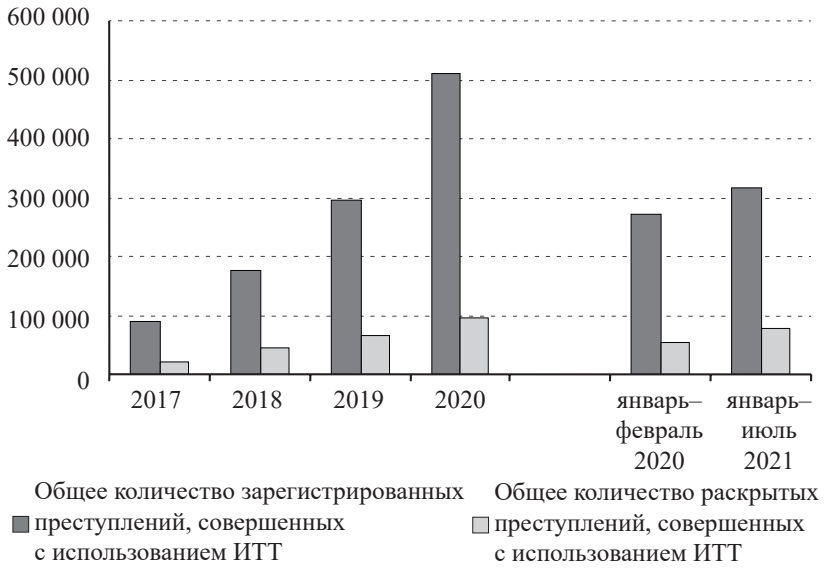

Рис. 1 Статистика преступлений, совершенных с использованием ИТТ

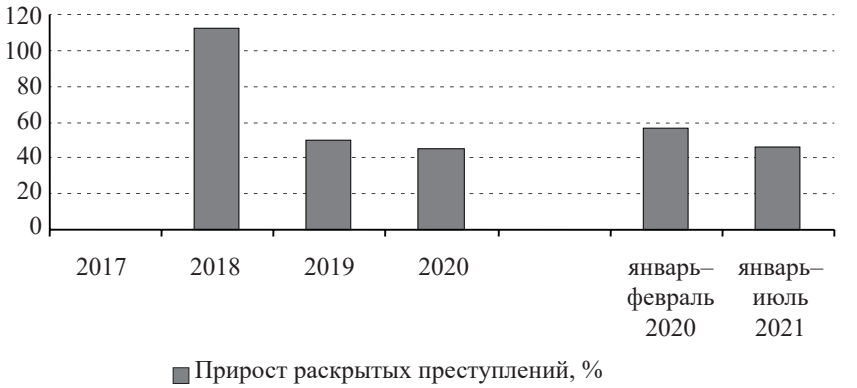

Рис. 2 Прирост раскрываемости преступлений, совершенных с использованием ИТТ, %

ные с использованием информационно-телекоммуникационных технологий (далее в рис. — ИТТ), увеличиваются очень быстрыми темпами. При этом, как видно на представленных ниже диаграммах, четко прослеживается низкая раскрываемость преступлений, рассматриваемой категории. Об этом свидетельствуют низкие показатели количества раскрытых преступлений, а также уменьшение прироста раскрываемости. Данный факт подтверждает одну из наших гипотез о неподготовленности правоохранительных органов к борьбе с преступлениями, совершенными с использованием информационно-телекоммуникационных технологий.

Также стоит отметить, что среди способов совершения преступлений, в сфере информационно-телекоммуникационных технологий, лидирующую позицию занимают преступления, совершенные посредством сети Интернет. Так, в 2019 г. преступления, совершенные с использованием сети Интернет составили 157,0 тыс., при общем количестве зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий — 294,4 тыс., что составляет почти половину. В 2020 г., это соотношение еще более увеличилось, так количество преступлений, совершенных с использованием сети Интернет составило 300,3 тыс., а общее количество зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий составило 510,4 тыс., т.е. доля преступлений, совершенных посредством сети Интернет составила больше половины от общего числа. Необходимо также учесть то, что показатель раскрываемости преступлений, совершенных с использованием сети Интернет, очень мал. За 2019 г. из 157,0 тыс. преступлений, раскрыто 35,1 тыс. (22,4 %), а в 2020 г. из 300,3 тыс. преступлений было раскрыто лишь 56,4 тыс., т.е. 18,8 %. Складывающаяся тенденция, дает неутешительный прогноз. Все это подтверждает нашу гипотезу, о том, что проблема раскрытия преступлений, совершенных с использованием сети Интернет существует, и вероятно, проблема кроется именно в том, что криминальные элементы оседают и укрываются в такой зоне сети Интернет, в которой правоохранители не могут реализовать свою функцию по борьбе с преступностью. Именно этой зоной и является темная часть Интернета, так называемый Даркнет. И это явление оказыва-

ется настоящей угрозой национального и международного характера, в борьбе с которой правоохранители пока не готовы.

Проработав криминалистическую литературу, посвященную вопросу темной сети, мы пришли к выводу, что в области криминалистики, и в Российском законодательстве, в целом, отсутствует единое понимание такого явления, как Даркнет несмотря на то, что многие авторы предпринимали попытки дать определение явлению Даркнет. Так, И.И. Сафиуллина и И.Р. Бегишев, в своей работе представили термин «теневой Интернет», как скрытую группу вебсайтов, доступную посредством специализированных браузеров [5, с. 286]. Более емкое определение Даркнета приводит Д.В. Жмуров, понимая под этим термином скрытую часть сети Интернет, которая состоит из взаимосвязанных зашифрованных туннелей, в которых пользователь остается полностью анонимным [6, с. 89]. Такое определение достаточно широко рассматривает и передает суть Даркнета. А.Г. Багдасарян в своей работе достаточно глубоко освятила явление Даркнет, углубившись в историю появления данного термина, а также, представив принцип работы сети Даркнет, в результате чего, автором предложен термин Darknet, под которым понимается скрытая сеть, полностью анонимная, в которой соединения происходят между доверенными узлами, так называемыми пирами, использующие нестандартные протоколы, при этом вся информация зашифровывается [7, с. 58]. Проанализировав, представленные авторами определения, можно сделать вывод об отсутствии единообразия в представленных формулировках. Кроме того, отметим, что отсутствует единая форма данного термина, так, часто встречающимися являются: англоязычная форма — DarkNet, Dark Web, русскоязычная форма — Даркнет, темная сеть, темный Интернет, глубокая сеть, теневой Интернет и т.д. Ввиду отсутствия общего и единого термина, мы предлагаем прийти к единому пониманию явления Даркнет в криминалистической науке. Разработанная дефиниция Даркнет будет отображать его важные черты, позволяющие построить дальнейшую концепцию исследования данного явления, как объекта криминалистики. Стоит иметь ввиду, что Даркнет, как пространство, пусть и виртуальное, имеет свои отличительные особенности, которые несут в себе совершенно иную криминалистически значимую информацию, так необходимую для построения частной криминалистической методики расследования преступлений, совершенных с его помощью.

Для того, чтобы прийти к единому пониманию того, что есть Даркнет, необходимо изучить этимологию данного слова, философскую составляющую, а также концепцию и принцип работы данного явления.

Слово Даркнет происходит от англ. DarkNet, что переводится как «темная сеть», также существует иная англоязычная форма — DarkWeb. Даркнет был разработан в 70-х гг. прошлого столетия, для обозначения сетей, изолированных от Арпанета, который в последующем эволюционировал в Интернет [7, с. 57]. Впервые термин «Даркнет» был использован в 2002 г. в книге сотрудников компании Microsoft, которая называлась «Даркнет и будущее распространения информации» [8, с. 273].

Немаловажное значение для понимания явления Даркнет, имеет философская составляющая. С философской точки зрения, возникновение Даркнета обусловлено стремлением людей к проявлению свободы духа и реализации творческих возможностей. Именно

так представляют себе пространство Даркнета трансгуманисты, считая, что создано данное пространство исключительно в благих целях. Анархопримитивисты же считают современные технологии противоестественными, и напротив, лишают человека свободы, делая его зависимым существом. Однако, в современных реалиях, Даркнет все же ассоциируется с криминальной составляющей. Необходимо учитывать, что сама сеть Даркнет не является противозаконной и общественно опасной, опасность представляет контент, размещенный в данной сети, и пользователи, использующие возможности Даркнета, для осуществления деятельности преступного характера. И все же, несмотря на разрозненность взглядов, главным преимуществом сети Даркнет является возможность сохранения анонимности, что привлекает преступников для избегания ответственности, будь то уголовной, будь то иной юридической, а также недопущения идентификации личности.

Мы обратились к зарубежной справочной литературе, а именно Кембриджскому словарю[2], который трактует «даркнет» как компьютерная сеть, использующая Интернет, но к которой могут присоединяться только те люди, у которых есть разрешение или необходимое программное обеспечение. Представленная в данном словаре концепция Даркнета заключается в скрытой организации анонимного и безопасного общения между людьми, и обменивания файлами друг с другом. Кроме того, мы обратились на сайт международной компании «Лаборатория Касперского», которая, на наш взгляд, является достаточно авторитетной компанией, работающей в сфере информационной безопасности. «Лаборатория Касперского» дает следующее определение Даркнета — это скрытая группа веб-сайтов, доступная только через специализированные браузеры[3].

Для того, чтобы более подробно исследовать Даркнет, как элемент глобальной сети, необходимо понять отличие Даркнета от своих собратьев. Всемирная сеть представляет собой виртуальное пространство, объединяющая в себе миллионное количество веб-сайтов, серверов и всевозможных баз данных. Если же представить Всемирную сеть в виде айсберга, то станет намного легче понять ее структуру. На поверхности «айсберга» находятся видимые, открытые и общедоступные веб-сайты, которые индексируются всем известными поисковыми системами, и посещение которых осуществляется с помощью популярных браузеров, таких как Google Chrome, например. Эта часть Всемирной сети называется поверхностным или открытым Интернетом, и составляет самую малую долю, приблизительно 5 % от общего объема [9, с. 18]. Та часть, так называемого айсберга, которая спрятана в глубине, «под водой», называется глубоким Интернетом. Данная часть Всемирной сети содержит преобладающую часть веб-ресурсов, которые, в свою очередь, не индексируются поисковыми системами. В глубоком Интернете размещаются сайты, защищенные какими-либо механизмами безопасности, например, защита паролями, кроме того, на просторах глубокого Интернета размещены страницы, которые недоступны для общего доступа, в целях защиты конфиденциальности пользователей сети, а также защиты таких сведений, как учетные записи мессенджеров и электронных почт, закрытые базы данных, пенсион-

[2] Cambridge Dictionary URL: https://dictionary.cambridge.org/dictionary/english/darknet?q=Darknet (дата обращения: 29.09.2021).

[3] Kaspersky. URL: https://www.kaspersky.ru/resource-center/threats/deep-web (дата обращения: 29.09.2021).

ные счета и т.п. На этом уровне глубокий Интернет не несет никакой угрозы безопасности компьютерам и их пользователям. Однако, чем глубже пользователь погружается в сеть, тем более опаснее становится контент, размещенный в данном пространстве. Именно здесь начинается теневой Интернет, являющийся самой нижней точкой «айсберга». Теневой Интернет очень хорошо спрятан в глубине Всемирной сети, и добраться до него может не каждый пользователь. Дело в том, что веб-сайты, размещенные в теневом Интернете, не только не индексируются поисковыми системами, но и для того, чтобы посетить данные сайты необходимы специализированное программное обеспечение и браузеры. Недоступность для обычных браузеров объясняется уникальными доменами сайтов. Самой главной особенностью Даркнета является применяемый принцип файлообмена. В данном случае применяется нестандартный метод, так называемое туннелирование трафика. Суть данного метода заключается в передачи сообщений между двумя объединенными сетями через транзитные сети, и что очень важно, данные сети, а также количество сетей, сгенерированны случайным образом. Кроме того, применяются такие меры сетевой безопасности, как анонимизирование. данном случае применяются такие технологии, как туннели и анонимные сети. Анонимные сети представляют собой систему прокси-серверов, которые функционируют путем создания цепочки из промежуточных соединений. Прокси-серверы, в свою очередь, выступают посредниками пользовательскими устройствами и сетью. По такому принципу устроена наиболее популярная сеть, используемая в сети Даркнет, сеть Tor (от англ. The Onion Router). Данная сеть надежно скрывает информацию о пользователях, в том числе местоположение. Анонимность в данной сети достигается благодаря использованию промежуточных узлов между пользователем и сервером, в результате чего, идентифицировать пользователя по IP- адресу становится практически невозможно [10, с. 217]. Принцип работы Tor основан на технологии «луковая» маршрутизация. Данная технология предоставляет пользователю приватную сессию, путем генерации случайной цепочки происхождения пакетов и шифрования информации [11, с. 64]. Отправляемые сообщения несколько раз шифруются и отправляются через несколько маршрутизаторов, каждый из которых удаляет слой шифра для того, чтобы открыть трассировочные инструкции и отследить последовательность выполнения команд, шифрует и отправляет на следующий маршрутизатор, где процедура повторяется. Таким образом, промежуточные маршрутизаторы не имеют доступа к информации ни об источнике, ни о пункте назначения, ни о содержании сообщения [12, с. 69].

Кроме браузера «Tor», к числу анонимайзеров и других средств сокрытия информации о пользователе, компьютере в частности, можно отнести следующее: анонимная сеть «I2P», которая скрывает IP-адрес пользователя; различные VPN-сервисы, с помощью которых возможно изменить место выхода в Интернет [13, с. 39].

Подведя итог, можно выделить ряд наиболее значимых признаков Даркнета, к ним мы относим: во-первых, Даркнет — это информационно-коммуникационная система, предназначенная для взаимодействия ее пользователей; во-вторых, с технологической точки зрения, Даркнет доступен посредством программного обеспечении, функционирующего по принципу «луковой маршрутизации», в

частности Tor, и его аналоги; в-третьих, Даркнет предоставляет пользователям полную анонимность, которая достигается за счет, шифрования информации.

Учитывая все вышесказанное, можно предложить следующую дефиницию Даркнет — это информационно-коммуникационная система, реализующая анонимизированную коммуникацию пользователей, посредством специализированного программного обеспечения. На наш взгляд, такая дефиниция полностью отображает сущность Даркнета, передавая его концепцию. В дальнейшем нами планируется исследование Даркнета, по классической схеме «от общего к частному». Первостепенно необходимо изучение специализированного программного обеспечения, осуществляющее выход в сеть Даркнет, в частности, виды программного обеспечения, его особенности и отличия от программного обеспечения для выхода в классический Интернет, технические характеристики. Кроме того, необходимо более подробное изучение браузеров и анонимайзеров, реализующих безликое существование пользователей в Даркнете, их разновидности и технические характеристики. Особенно важно, проведение анализа преступного контента, размещенного в сети Даркнет. Данный подход, возможно, позволит получить новые источники для построения элементов криминалистической характеристики, которая послужит основой для построения частных криминалистических теорий расследования преступлений, совершенных с использованием новых информационных технологий, а именно посредством сети Даркнет. О необходимости дополнения традиционной эмпирической базы, служащей источником для построения элементов криминалистической характеристики, ранее уже отмечалось [14, с. 72].

Таким образом, анализ статистических данных, представленных МВД России, о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий, позволяет сделать вывод о том, что преступления, совершенные с использованием сети Интернет, являются наиболее популярными. В свою очередь, уровень раскрываемости преступлений, рассматриваемой категории, говорит о том, что проблема раскрытия преступлений совершенных с использованием сети Интернет существует, и заключается, вероятно, в том, что криминальные элементы оседают и укрываются в теневой зоне сети Интернет, в которой правоохранители не могут реализовать свою функцию по борьбе с преступностью, представленная зона и есть сеть Даркнет, которая по праву является настоящей угрозой национального и международного характера, в борьбе с которой правоохранители не обладают криминалистически подкрепленной базой.

Предложенная нами дефиниция Даркнет позволит построить концепцию исследования новой среды совершения преступлений и получить новые источники для построения элементов криминалистической характеристики преступлений, совершенных с использованием информационно-телекоммуникационных технологий нового уровня. Что, в свою очередь, послужит основой построения частной криминалистической теории расследования преступлений, совершенных с использованием сети Даркнет.

СПИСОК ИСТОЧНИКОВ

1. Галий А.А. "Даркнет" как угроза национальной безопасности Российской Федерации / А.А. Галий, И.В. Слюсарь // Вестник науки. — 2018. — Т. 1, № 9 (9). — С. 204–205.

2. Куфлева В.Н. Проблемы квалификации преступлений, связанных с использованием шифрования информации и обеспечением анонимности в сети Интернет / В.Н. Куфлева, А.И. Литовченко. — DOI 10.24158/pep.2021.9.13 // Общество: политика, экономика, право. — 2021. — № 9 (98). — С. 80–83.

3. Мухин С.М. Преступления в сети Darknet: краткая характеристика, проблемы противодействия / С.М. Мухин // Альманах молодого исследователя. — 2018. — № 5. — С. 110–114.

4. Александров А.Г. Использование сети даркнет при подготовке и совершении преступлений / А.Г. Александров, А.А. Сафронов. — DOI 10.35750/2071-8284-2021-1-156-160 // Вестник Санкт-Петербургского университета МВД России. — 2021. — № 1 (89). — С. 156–160.

5. Сафиуллина И.И. Теневая паутина как средство подготовки к совершению преступлений / И.И. Сафиуллина, И.Р. Бегишев // Научные исследования: фундаментальные и прикладные аспекты — 2021: сб. науч. тр. / отв. ред. И.И. Фролова. — Казань, 2021. — С. 286–288.

6. Жмуров Д.В. Даркнет как ускользающая сфера правового регулирования / Д.В. Жмуров // Сибирские уголовно-процессуальные и криминалистические чтения. — 2020. — № 1 (27). — С. 89–98.

7. Багдасарян А.Г. Даркнет: особенности и история / А.Г. Багдасарян // Конкурс молодых ученых: сб. ст. VI Междунар. науч.-исслед. конкурса, Пенза, 20 нояб. 2020 г. / отв. ред. Г.Ю. Гуляев. — Пенза, 2020. — С. 56–58.

8. Трансформация права в цифровую эпоху / под ред. А.А. Васильева. — Барнаул: Изд-во Алт. гос. ун-та, 2020. — 432 с.

9. Петухов А.Ю. Современные тенденции использования средств теневого Интернета при совершении преступлений в сфере незаконного оборота наркотиков / А Ю. Петухов, К.С. Куликов. — DOI 10.51980/2686-939X_2019_1_17 // Научный компонент. — 2019. — № 1 (1). — С. 17–23.

10. Фролов А.А. Исследование механизмов распространения запрещенного содержимого в Darknet / А.А. Фролов, Д.С. Сильнов. — DOI 10.25559/SITITO.2017.4.444 // Современные информационные технологии и ИТ-образование. — 2017. — Т. 13, № 4. — С. 216–224.

11. Симаков А.А. Анонимность в глобальных сетях / А.А. Симаков // Научный вестник Омской академии МВД России. — 2017. — № 2 (65). — С. 62–65.

12. Полунина А.В. Даркнет: по ту сторону Интернета / А.В. Полунина, Р.М. Магомедов // Академический журнал Западной Сибири. — 2019. — Т. 15, № 3 (80). — С. 69–70.

13. Апкаев Д.М. Преступления, совершенные неустановленными лицами с использованием анонимайзеров и VPN-сервисов: проблемы противодействия / Д.М. Апкаев, Н.М. Никишкин // Пенитенциарное право: юридическая теория и правоприменительная практика. — 2021. — № 1 (27). — С. 39–41.

14. Васильева Н.А. Анализ цифровых платформ в сфере незаконного оборота наркотиков для построения криминалистической характеристики данного вида преступлений / Н.А. Васильева // Юридическая наука. — 2020. — № 2. — С. 71–76.

REFERENCES

1. Galiy A.A. "Darknet" as a Threat to the National Security of the Russian Federation. *Vestnik nauki = Herald of Science,* 2018, vol. 1, no. 9, pp. 204–205. (In Russian).

2. Kufleva V.N., Litovchenko A.I. Problems of Qualification of Crimes Related to the Use of Information Encryption and Ensuring Anonymity on the Internet. *Obshchestvo: politika, ekonomika, pravo = Society: Politics, Economics, Law,* 2021, no. 9, pp. 80–83. (In Russian). DOI: 10.24158/pep.2021.9.13.

3. Mukhin S.M. Crimes in the Darknet Network: Brief Description, Problems of Counteraction. *Al'manakh molodogo issledovatelya = Almanac of a Young Researcher*, 2018, no. 5, pp. 110–114. (In Russian).

4. Aleksandrov A.G., Safronov A.A. Use of Darknet to Prepare and Commit Crimes. *Vestnik Sankt-Peterburgskogo universiteta MVD Rossii = Saint-Petersburg University of Ministry of Internal Affairs of Russia Bulletin*, 2021, no. 1, pp. 156–160. (In Russian). DOI: 10.35750/2071-8284-2021-1-156-160.

5. Safiullina I.I., Begishev I.R. The ShadowWweb as a Means of Preparing to Commit Crimes. In Frolova I.I. (ed.). *Scientific Research: Fundamental and Applied Aspects — 2021.* Kazan, 2021, iss. 1, pp. 286–288. (In Russian).

6. Zhmurov D.V. Darknet as an Elusive Sphere of Legal Regulation. *Sibirskie ugolovno-protsessual'nye i kriminalisticheskie chteniya = Siberian Criminal Procedure and Criminalistic Readings,* 2020, no. 1, pp. 89–98. (In Russian).

7. Bagdasaryan A.G. Darknet: Features and History. In Gulyaev G.Yu. (ed.). *Competition for Young Scientists. Collected Papers Based on the Materials of the 6th International Scientific Competition, Penza, November 20, 2020.* Penza, 2020, pp. 56–58. (In Russian).

8. Vasiliev A.A. (ed.). *Transforming Law in the Digital Age*. Barnaul, Altai State University Publ., 2020. 432 p.

9. Petukhov A.Yu., Kulikov K.S. Modern Trends in the Use of Means of the Dark Internet in Commission of Crimes in the Sphere of Illegal Drug Trafficking. *Nauchnyi komponent = Scientific Component,* 2019, no. 1, pp. 17–23. (In Russian). DOI: 10.51980/2686-939X_2019_1_17.

10. Frolov A.A., Silnov D.S. Research of Prohibited Content Distribution Mechanisms in the Darknet. *Sovremennye informatsionnye tekhnologii i IT-obrazovanie = Modern Information Technology and IT-education,* 2017, vol. 13, no. 4, pp. 216–224. (In Russian). DOI: 10.25559/SITITO.2017.4.444.

11. Simakov A.A. Anonymity in Global Networks. *Nauchnyi vestnik Omskoi akademii MVD Rossii = Scientific Bulletin of the Omsk Academy of the MIA of Russia,* 2017, no. 2, pp. 62–65. (In Russian).

12. Polunina A.V. Magomedov R.M. Dartnet: on the Other Side of the Internet. *Akademicheskii zhurnal Zapadnoi Sibiri = Academic Journal of West Siberia*, 2019, vol. 15, no. 3, pp. 69–70. (In Russian).

13. Apkaev D.M., Nikishkin N.M. Crimes Committed by Unidentified Persons Using Anonymizers and VPN Services: Problems of Counteraction. *Penitentsiarnoe pravo: yuridicheskaya teoriya i pravoprimenitel'naya praktika = Penal Law: Legal Theory and Law Enforcement Practices,* 2021, no. 1, pp. 39–41. (In Russian).

14. Vasilieva N.A. Analysis of Digital Platforms in the Sphere of Illegal Drug Trade for Making Up the Forensic Characteristic of Such Crimes. *Yuridicheskaya nauka = Legal Science,* 2020, no. 2, pp. 71–76. (In Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Протасевич Александр Алексеевич — доктор юридических наук, профессор, заслуженный юрист Российской Федерации и Республики Бурятия, почетный работник Министерства образования, заслуженный профессор Байкальского государственного университета, Байкальский государственный университет, г. Иркутск, Российская Федерация.

Скрябикова Юлия Борисовна — аспирант, кафедра криминалистики, судебных экспертиз и юридической психологии, Институт юстиции, Байкальский государственный университет, г. Иркутск, Российская Федерация.

INFORMATION ABOUT THE AUTHORS

Aleksander A. Protasyevich — Doctor of Law, Professor, Honorary Lawyer of the Russian Federation and the Buryat Republic, Honorary Worker of the Ministry of Education, Honorary Professor of Baikal State University, Baikal State University, Irkutsk, the Russian Federation.

Yulia B. Skryabikova — Ph.D. Student, Department of Criminalistics, Court Forensic Expertise and Legal Psychology, Institute of Justice, Baikal State University, Irkutsk, the Russian Federation.

Поступила в редакцию / Received 20.08.2021
Одобрена после рецензирования / Approved after reviewing 14.09.2021
Принята к публикации / Accepted 09.12.2021
Дата онлайн-размещения / Available online 22.12.2021