ОСОБОЕ МНЕНИЕ

УДК 343.9

Д.В. Жмуров

ДАРКНЕТ КАК УСКОЛЬЗАЮЩАЯ СФЕРА ПРАВОВОГО РЕГУЛИРОВАНИЯ

В статье изучены отдельные вопросы, касающиеся криминальной деятельности в сети Даркнет, а также особенностей его использования различными категориями преступников. Для этих целей был проведен контент-анализ содержания соответствующих интернет-ресурсов, размещенных как в открытом, так и скрытом сегментах Интернет. Проведенное исследование позволило выделить и описать как минимум десять наиболее распространенных криминальных ниш в Даркнет. Вместе с тем, очевидно, что немалая часть проанализированных видов общественно опасной деятельности представлена и в традиционном Интернет, что свидетельствует о переоцененности криминального значения темной сети. Более того, установлено, что большая часть преступлений совершаются в обоих сегментах всемирной паутины синхронно.

Ключевые слова: киберпреступность, Даркнет, темный Интернет, цифровая криминология.

D.V. Zhmurov

DARKNET AS AN ELUSIVE SPHERE OF LEGAL REGULATION

The author examines some aspects of criminal activities in the Darknet, and its use by different categories of criminals. Content-analysis of corresponding Internet resources both in the open and the hidden segments of the Internet allowed the author to single out and describe at least ten most common criminal niches in the Darknet. At the same time, it is obvious that a large part of the analyzed types of publically dangerous activities is also present in the traditional Internet, which shows that the significance of the Darknet for criminal activities is overrated. Moreover, the author states that most crimes are committed in both segments of the web simultaneously.

Keywords: cybercrime, Darknet, dark Internet, digital criminology.

Даркнет кардинально изменил современную преступность. Под этим термином понимается скрытая часть сети Интернет, состоящая из связанных между собой виртуальных и зашифрованных туннелей в которых пользователь остается полностью анонимным.

Сегодня Даркнет – это теневой рынок с многомиллионными оборотами. Он похож на открытую сеть и тоже состоит из сайтов, форумов и торговых площадок [1]. Продажа наркотических веществ, оружия, вредоносных про-

грамм, отмывание средств и экстремальная порнография стали неотъемлемой его частью. Все это происходит буквально на глазах у общества и правоохранительной системы. Приходится констатировать тот факт, что даркнет является ускользающей сферой правового регулирования и государство не в состоянии защитить цифровые права граждан в этой области. Традиционная преступность стремительно дигитализируется, пытаясь отыскать свою нишу в глобальном телекоммуникационном пространстве. Киберпреступность стала одной из наиболее актуальных мировых проблем [2]. Криминальные группировки используют Даркнет для пропаганды, рекрутинга и наращивания финансовой мощи. Там же осуществляется торговля людьми. Утверждается, что купить можно как живого человека, так и цифровую личность. Только в США уже более 60 млн. людей пострадали от электронных краж идентичности[1]. Объем сети Даркнет, по разным данным, составляет около 1% от размера основного Интернет [3].

Таким образом, с полной уверенностью можно утверждать о формировании нового криминального феномена именуемого Даркнет, символизирующего начало массовой «цифровой миграции» преступности из реального измерения в виртуальное. Особо актуально и то, что Даркнет до настоящего времени не получил всесторонней и адекватной научной оценки. Именно эти доводы подчеркивают универсальность проблемы и необходимость реагировать на неё уже сейчас.

На чрезвычайную актуальность вопроса указывают следующие моменты.

Во-первых, в преступности происходят глобальные процессы трансформации, по-сути меняется ее парадигма: криминальная среда уходит в цифровой мир. Даркнет стал отражением этих сложных процессов и для понимания эволюционного пути преступности необходимо углубленное изучение этого явления.

Во-вторых, Даркнет представляет глобальную угрозу безопасности, он скрывает и упрощает многообразные формы криминальной активности, гарантируя преступникам анонимность, существенно снижая потенциал раскрываемости отдельных преступлений [4]. Число незаконных транзакций в этой сети, по оценкам компании Chainalysis, только в биткоинах может достичь 1 млрд. долларов в 2019 г., что отражает востребованность данного Интернет-сегмента.

В-третьих, несмотря на растущий исследовательский интерес, Даркнет до настоящего времени не получил всесторонней и исчерпывающей научной оценки. Фундаментальных исследований, описывающих особенности русскоязычного Даркнет пока не выполнялось.

Эти аргументы подчеркивают необходимость скорейшего проведения исследований данного явления в рамках цифровой криминологии.

При подготовке настоящей статьи было проведено аналитическое исследование научных материалов по заявленной проблеме. Для первичного анализа были использованы ключевые слова «Даркнет», «Darknet», «Даркверб», «Тене-

[1] United States; Congress; House; Committee on Ways and Means (2018). Protecting Children from Identity Theft Act: report (to accompany H.R. 5192) (including cost estimate of the Congressional Budget Office).

вая сеть», «Темный Интернет». Поиск осуществлялся на базе портала E-library с учетом морфологии с последующей ручной обработкой результатов. Проведенный анализ позволил сделать несколько выводов относительно современного состояния исследований в этой области:

1. Научное сообщество не уделяет достаточного внимания поставленной проблеме, даже несмотря на резкое увеличение объема Даркнет и стремительного роста его популярности среди традиционных пользователей Интернет. Из 279 отобранных источников указанной тематики не было обнаружено ни одной тематической монографии. Среди публикаций отмечены: 182 статьи, 97 тезисов выступлений, 4 монографии по экономике, затрагивающие отдельные аспекты Даркнет. Подавляющее большинство работ датированы 2017 г. (51 работа или 18%), 2018 г. (119 работ или 43%) и 2019 г. (до октября 87 работ или 31%). То есть научная проблема еще только конкретизируется.

2. Значительная доля исследований охватывает отдельные вопросы заявляемой темы. Немало публикаций посвящены механизму транзакций в криптовалюте, технологии блокчейна, биткоину и проч. (51 или 18%). На втором месте по частоте актуальных разработок находятся различные аспекты оборота наркотических веществ в Даркнет (38 или 14%). Третьей темой, вызывающей интерес исследователей, стала дискуссия об информационной, экономической и кибернетической безопасности и современной роли Даркнет (31 или 11%). В 7 % или 19 работах рассматриваются вопросы экстремизма и кибертерроризма. Немного меньше исследований затрагивают криминалистические вопросы расследования отдельных преступлений, совершенных в Даркнет или с использованием криптовалюты (18 или 6 %). Остальные материалы посвящены многочисленным проблемам изучения «темного Интернет» или эта тема упоминается вскользь (в рамках политологии, языкознания, кибернетики и проч.). Таким образом, публикационный пул разрознен частными исследованиями без фундаментального и системного осмысления сложившейся ситуации. Всего 14,7% исследований целенаправленно изучают Даркнет, как социокриминальный феномен (напр., Галий А.А., Слюсарь И.В. «Даркнет» как угроза национальной безопасности Российской Федерации. 2018; Мазур А.А. Актуальные проблемы предупреждения преступности в социальной сети Даркнет. 2018; Полунина А.В., Магомедов Р.М. Даркнет: по ту сторону Интернета. 2019 и другие).

В зарубежной научной среде эта проблема обсуждается значительно шире и вынесена на повестку дня. К примеру, за последние годы опубликованы фундаментальные исследования данной темы: Гаяр Л. Даркнет: геополитика и применение (2018); Сенкер К. Киберпреступность и темная сеть: раскрытие преступного мира Интернет (2016); Мартин Д. Наркотики в темной сети: как криптомаркеты трансформируют мировую торговлю наркотиками (2014); Ласика Дж. Даркнет: война Голливуда против цифрового поколения (2005) и т.д. Государственные власти и исследователи за рубежом уделяют немалое внимание проблеме контроля над сетью Даркнет. Хотя и признается, что значительная часть этой теневой структуры безвредна, некоторые прокуроры и правительственные учреждения США обеспокоены тем, что эта технология является хорошим убежищем для преступности. В Америке действуют специализиро-

ванные мониторинговые центры, отслеживающие информацию об анонимных веб-ресурсах и даркнет-сервисах (напр., DeepDotWeb, All Things Vice). В 2017 г. исследовательской службой Конгресса США впервые был опубликован обширный отчет о темной сети, в котором аналитики констатировали растущий интерес ученых, сотрудников полиции и политиков к Даркнет, оценили финансовый объем и перспективы Даркнет.

В ходе проведенного исследования была осуществлена попытка сегментирования теневого рынка Даркнет. Следует отметить, что немалая часть проанализированных видов деятельности представлена и в традиционном Интернет, что свидетельствует о переоцененности криминального значения темной сети. Более того, большая часть преступлений совершаются в обоих сегментах всемирной паутины синхронно. К примеру, в даркнет покупаются данные краденных платежных карт, а техника оплачивается уже на «белых» сайтах (в «Клирнете»). В этом смысле Даркнет и классический Интернет дополняют друг друга.

Итак, были обнаружены, выделены и описаны следующие формы нелегальной (полулегальной) активности, не исключающие уголовно-правовой квалификации:

– оборот наркотических веществ (прекурсоров, сырья, оборудования и технологий их производства). Вероятно, это одна из наиболее распространенных практик темного Интернета. Бытует мнение о том, что российская торговая площадка «Гидра» стала мировым лидером по продаже наркотиков [5]. Россия в настоящее время занимает второе место в мире по числу пользователей даркнета в части оборота психоактивных веществ [6].

Всего на «Гидре» зарегистрировано 2,5 миллиона аккаунтов, 393 000 из них совершили за все время хотя бы одну покупку. Совокупный оборот площадки с 2016 по 2019 гг. составил 64,7 млрд. руб. или приблизительно 126,135 биткоинов [7]. По официальным данным, озвученным руководителем подразделения по контролю за оборотом наркотиков МВД РФ В. Хмельницким, каждое десятое преступление в интернет связано с оборотом наркотических веществ [8]. По сведениям зарубежных исследований около 10% наркопотребителей приобретали психостимулирующие вещества на анонимных рынках сети Даркнет [9].

– Оборот официальных или поддельных документов, государственных наград, штампов, печатей, дипломов и других полиграфических материалов (голограммы, справки, страховые бланки, акцизы). Формы осуществления данной деятельности разнообразны. Зачастую предлагаются документы, отпечатанные в кустарных условиях. Цена варьируется в зависимости от качества печати, к примеру, стоимость свидетельства о регистрации транспортного средства составляет от 11 до 15 тыс. руб., заполненная ПТС на автомобиль – 23 тыс. руб., нотариальная доверенность (заполненная) – 18 тыс. руб. и проч. Несколько реже продаются «оригинальные» бланки документов, отпечатанные в крупных типографиях (как правило, в Китае). Еще одним способом получения документов государственного образца являются различные формы подмены людей. Если цена поддельного паспорта начинается от 100 тыс. руб., то такая

услуга на порядок дороже (доходит до полумиллиона рублей). Ее суть заключается в том, что, к примеру, в органы ФМС обращается «подставной» человек (дроп), не имеющий кредитов, судимостей, выездов за границу, ведущий тихий и закрытый образ жизни. Дроп, якобы, теряет паспорт и пишет соответствующее заявление, а при оформлении нового документа вместо его фотографии коррумпированным сотрудником подкладывается фото заказчика. Услуга действует непродолжительное время, приблизительно через год дроп вновь напишет заявление об утере, но за этот год заказчик может успеть оформить загранпаспорт, ИНН, водительское удостоверение и проч.

– Криминальные услуги и иные деяния в сфере IT-индустрии. Это могут быть DDoS атаки, т.е. создание избыточного траффика и перегрузка атакуемого сайта; взлом электронной почты, интернет-сайтов и аккаунтов социальных сетей; компрометация и создание негативной репутации, разработка и продажа вредоносных программ; спам, флуд, продажа выделенных серверов для преступной деятельности в зарубежном интернет, продажа и массовый фарминг аккаунтов, кража баз данных, криптовалюты; обеспечение анонимности и безопасности какой-либо рискованной операции; обеспечение мошеннических схем ресурсами ip-телефонии и проч. Министр внутренних дел В. Колокольцев заявил о растущем масштабе угроз, связанных с использованием ip-телефонии, пояснив, что «преступники научились подменять подлинные телефонные номера кредитных организаций, государственных служб, выдавая себя за их работников»[2]. В сети вполне официально работают сервисы по подмене номера телефона, например Narayana.im

– Оборот орудий, технических средств совершения преступлений (продажа огнестрельного и травматического оружия, оборудования для скимминга, т.е. накладных элементов на банкоматы для кражи информации; прошитых POS-терминалов, сохраняющие в памяти track-данные и пин-код клиента, реализация код-грабберов для автоугонщиков; специальных средств, предназначенных для негласного получения информации; тайников для перевозки наркотических средств, замаскированных под обычные вещи; технических решений для шоп-лифтинга, в т.ч. различного рода глушилок, отмычек, деактиваторов меток, экранирующих материалов. Также продаются смартфоны, подготовленные для анонимной работы; wi-fi роутеры с настроенными TOR и VPN, аккаунты каршеринговых автомобилей, оборудование для нелегального приема и декодирования спутникового сигнала и т.д.).

– Офф-лайн услуги криминального характера, осуществляемые не в сети. Среди них отметим: давление на человека различной интенсивности (причинение мелких неудобств, поджог автомобиля от 100 тыс. руб., расстрел из травматического оружия от 100 тыс. руб. и проч.); удаление информации о судимости из базы данных ИЦ ГИАЦ МВД России – 300 тыс. руб.; переквалификация уголовной статьи на менее тяжкую (от 200 тыс. руб.). Встречаются и более экзотические объявления, например, услуги промышленного шпионажа (от

[2] Колокольцев назвал новой угрозой мошенничество с использованием IP-телефонии [эл.ресурс] // URL: https://tass.ru/obschestvo/7070806 (дата обращения 8.01.2020).

150 тыс. руб.); устранение объекта (от 200 тыс. руб.); отбывание тюремного срока вместе реального обвиняемого (по договоренности); запись на прием к врачам и т.д. Сколько из этих объявлений являются фейковыми предположить сложно.

– Фрод, как вид мошенничества в области информационных технологий, в частности, несанкционированные действия и неправомерное пользование ресурсами и услугами. Сюда включают кардинг и рефандинг. Кардеры это те, кто ворует деньги с чужих банковских счетов и обналичивают их самыми разными способами, а рефандеры это те, кто возвращает собственные деньги за купленные якобы «некачественные» вещи у магазинов, оставаясь при этом и с деньгами и с товаром. В Даркнет, как и в традиционном Интернет, достаточно много контента, посвященного теме фрода. У кардеров - это продажи мата (самих пластиковых носителей), различных услуг, оплаченных такими картами (отелей, билетов на самолет с дисконтом 30-50%), сбыт карженной техники, т.е. незаконно приобретенной на чьи-то средства и перепродаваемой со значительной скидкой (нередко это мошенничества и реального товара нет). У рефандеров, имитирующих недоброкачественность товара и возвращающих уплаченные за него деньги - продажа полученных таким способом вещей. Различают несколько видов рефанда: а) возмещение стоимости товара без его возврата продавцу (refund), то есть деньги плюс товар; б) замена аналогичным продуктом (replace), то есть два товара; в) денежная компенсация и товар (refund & replace), то есть два товара плюс деньги [10].

– Рынок труда, связанный с незаконной деятельностью охватывает сотни объявлений на форумах с различными предложениями о трудоустройстве и сотрудничестве (зачастую это предложения работодателей, связанные с торговлей наркотическими средствами. В этой сфере востребованы более 14 профессий, среди которых складмены, диспетчеры, закладчики, трафаретчики, кадровики и т.д. Кроме того, постоянно требуются обнальщики (в сфере легализации черных и серых денежных средств), холдеры (ложные покупатели), лица, осуществляющие «вбив в шопах» (оформляющие покупку в интернет-магазине на холдера), вебкам-модели (таких девушек ищут владельцы порностудий), партнеры по датинг-скаму (аферисты в сфере удаленных знакомств), курьеры, it-работники (модераторы, копирайтеры, программисты, эксперты, маркетологи, оптимизаторы), дроповоды (или рекрутеры, т.е. лица подбирающие персонал для нелегальных операций) и проч.

– финансовые и консалтинговые услуги. Первые представляют собой различные формы обмена валют, биткоин-миксеры, как средство анонимизации платежей в криптовалюте. Механизм работы миксера заключается в том, что средства клиента дробятся на множество частей, смешиваются с деньгами других лиц, а потом, после многочисленных переводов, возвращаются ему на кошелек. Помимо этого, можно встретить предложения о продаже готовых компаний (ООО, ИП), зарегистрированных на подставных лиц, оформлении дебетовых карт или кредитов по подложным документам, продаже взломанных аккаунтов PayPal для совершения анонимных покупок и проч. Сюда же можно отнести манипуляции с электронными платежными средствами (восстановле-

ние или обналичивание с сим-карт, идентификация нелегальных интернет кошельков или продажа готовых, работа с блокированными электронными счетами для получения доступа).

Консалтинговые услуги напоминают своеобразные франшизы посвященные заработку в Интернет, как рискованные, так и легальные (по утверждению рекламодателей). Проводится обучение кардингу, фишингу, поиску вебкам-моделей, рассылкам, анонимному серфингу, скрытому майнингу, дроповодству, взлому vk, обналичиванию денег, бонус-хантингу, датинг скам, заработку на социальных программах помощи населению, генерации траффика, беттингу (получению дохода на спортивных ставках), инфо-скаммингу (созданию псевдоэкспертов в социальных сетях и мессенджерах, которые учат зарабатывать). Курсы обучения проводятся дистанционно или очно, некоторые «франчайзи», помимо информационных материалов, гарантируют доведение клиента до первого профита (прибыли).

– Услуги связанные с нарушением неприкосновенности частной жизни (детализация звонков, наблюдение за объектом, получение конфиденциальной информации о лице от операторов мобильных связи, банковских и государственных учреждений).

– Сообщества лиц страдающих сексуальными парафилиями, например форумы педофилов. Там проходит дискуссии и обсуждения на тему как лучше совратить собственную дочь без серьезных последствий и чтобы супруга об этом догадывалась. Девочек педофилы называют «белками». «Белка» - ребенок до 10-12 лет. Некоторые пишут в своих откровениях, что начали развращать своих детей с 2-5 лет, охотно делятся опытом с остальными[3].

– Прочие ресурсы (сайты экстремистских организаций, хакерские торговые площадки, черные биржи криптовалюты и т.д.)

Очевидно, что все вышеперечисленное можно обнаружить и в обычном Интернет. Вместе с тем, Даркнет все же более криминализирован и содержит немалое число ресурсов, нарушающих уголовные законы. Само его существование некоторые авторы оценивают, как угрозу национальной безопасности России [11]. Высказывается мнение о том, что большинство из этих сайтов – скам, мошенничество и попытка обмануть наивного пользователя. Есть прямо противоположные точки зрения. Таким образом, Даркнет, как социокультурный феномен является малоизученным и противоречивым явлением. В связи с этим необходимо следующее:

1. Системное описание криминальных компонентов сети Даркнет (анализ русскоязычных интернет ресурсов и уголовно-правовая оценка их деятельности, контент-анализ объявлений на крупнейших черных рынках, ценовое сегментирование криминальных услуг и вычисление усредненных показателей их стоимости, оценка заполненности различных криминальных ниш).

[3] Форум для педофилов [эл.ресурс] // Мониторинговый центр по выявлению опасного и запрещенного законодательством контента. URL: http://www.pedofilov.net/news/russia/forum-dlya-pedofilov-/ (дата обращения 6.01.2020).

2. Исследование осведомленности различных возрастных групп населения относительно существования Даркнет, выявление предпочтительных форм и целей его использования, выяснение персонального отношения респондентов к этому явлению.

3. Сравнительно-правовой анализ законодательства и правоприменительной практики в области противодействия киберпреступности в Даркнет (опыт США, отдельных стран Евросоюза, Китая).

4. Разработка методик расследования преступных деяний, совершенных в сети Даркнет и (или) при помощи ее использования.

5. Разработка основ комплексной программы профилактики анонимной преступности существующей в Даркнет, как неотъемлемого раздела цифровой криминологии [12].

Список использованной литературы

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

2. Протасевич А.А. Борьба с киберпреступностью, как актуальная задача современной науки / А.А. Протасевич, Л.П. Зверянская // Криминологический журнал Байкальского государственного университета экономики и права. – 2011. – № 3. – С. 28–33.

3. Иксанов Р.А. Защита прав граждан от посягательств в сети Даркнет / Р.А. Иксанов, Г.С. Слепов // Международный журнал гуманитарных и естественных наук. – 2018. – № 4. – С. 271–273.

4. Блокчейн в цифровой криминологии: постановка проблемы / А.П. Суходолов, Е.А. Антонян, М.В. Рукинов [и др.]. – DOI 10.17150/25г00-4255.2019.13(4).555-563 // Всероссийский криминологический журнал. – 2019. – Т. 13, № 4. – С. 555–563.

5. Дорожный А. Вся эта дурь: Исследование о том на чем сидит Россия / А. Дорожный, А. Хачатурянц // Проект медиа. – 2019. – URL: https://www.proekt.media/research/narkotiki-v-darknete/ (дата обращения: 3.12.2020).

6. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции / С.В. Иванцов, Э.Л. Сидоренко, Б.А. Спасенников [и др.]. – DOI 10.17150/2500-4255.2019.13(1).85-93 // Всероссийский криминологический журнал. – 2019. – Т. 13, № 1. – С. 85–93.

7. Криптовалюты: легальные и криминально-теневые аспекты оборота / В.В. Дорофеева, Л.А. Каверзина, Д.В. Жмуров [и др.]. – DOI 10.17150/2500-4255.2019.13(6).884-894 // Всероссийский криминологический журнал. – 2019. – Т. 13, № 6. – С. 884–894.

8. Петров И. Синтетическая угроза / Петров И. // Российская газета. – 2019. – 6 февр. – URL: https://rg.ru/2019/02/06/kazhdoe-desiatoe-prestuplenie-v-internete-sviazano-s-narkotikami.html (дата обращения: 3.12.2020).

9. Goodman M. Future Crimes: Inside the Digital Underground and the Battle for Our Connected World / M. Goodman. – New York : Doubleday, 2015. – 393 p.

10. Судиловская Е. На грани обмана: как заработать на рефанде / Е. Судиловская // Navika. – URL: https://navika.pro/rassledovaniye/posts/na-grani-obmana-kak-zarabotat-na-refande (дата обращения: 4.12.2020).

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

12. Судакова Т.М. Осмысление будущего криминологии: обзор современных тенденций / Т.М. Судакова, В.А. Номоконов. – DOI 10.17150/2500-4255.2018.12(4).531-540 // Всероссийский криминологический журнал. – 2018. – Т. 12, № 4. – С. 531–540.

References

1. 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).

2. Protasyevich A.A., Zveryanskaya L.P. Fighting Cybercrimes as an Urgent Task for Contemporary Research. *Kriminologicheskii zhurnal Baikal'skogo gosudarstvennogo universiteta ekonomiki i prava = Criminology Journal of Baikal National University of Economics and Law*, 2011, no. 3, pp. 28–33. (In Russian).

3. Iksanov R.A., Slepov G.S. Protection of the Rights of Citizens From Encourages in the Network of Darknet. *Mezhdunarodnyi zhurnal gumanitarnykh i estestvennykh nauk = International Journal of Humanities and Natural Sciences*, 2018, no. 4, pp. 271–273. (In Russian).

4. Sukhodolov A.P., Antonyan E.A., Rukinov M.V., Shamrin M.Yu., Spasennikova M.G. Blockchain in digital criminology: problem statement. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2019, vol. 13, no. 4, pp. 555–563. DOI: 10.17150/2500-4255.2019.13(4).555-563. (In Russian).

5. Dorozhnyi A., Khachaturyants A. All this junk: Studying what Russia is high on. *Proekt media = Project Media*, 2019. Available at: https://www.proekt.media/research/narkotiki-v-darknete/. (In Russian).

6. Ivantsov S.V., Sidorenko E.L., Spasennikov B.A., Berezkin Yu.M., Sukhodolov Ya.A. Cryptocurrency-related crimes: key criminological trends. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2019, vol. 13, no. 1, pp. 85–93. DOI: 10.17150/2500-4255.2019.13(1).85-93. (In Russian).

7. Dorofeeva V.V., Kaverzina L.A., Zhmurov D.V., Krasnova T.G., Burakov V.I. Cryptocurrencies: legal and shadow-criminal aspects of turnover. Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology, 2019, vol. 13, no. 6, pp. 884–894. DOI: 10.17150/2500-4255.2019.13(6).884-894. (In Russian).

8. Petrov I. Synthetic threat. *Rossiiskaya Gazeta*, 2019, February 6. Available at.: https://rg.ru/2019/02/06/kazhdoe-desiatoe-prestuplenie-v-internete-sviazano-s-narkotikami.html. (In Russian).

9. Goodman M. *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*. New York, Doubleday, 2015. 393 p.

10. Sudilovskaya E. On the verge of deception: how to make money on refund. *Navika*. Available at: https://navika.pro/rassledovaniye/posts/na-grani-obmana-kak-zarabotat-na-refande (In Russian).

11. Galii A.A., Slyusar I.V. Darknet, as a threat to the national security of the Russian Federation. *Vestnik nauki = Bulletin of Science*, 2018, vol. 1, no. 9, pp. 204–205. (In Russian).

12. Sudakova T. M., Nomokonov V. A. Understanding the future of criminology: an overview of current trends. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2018, vol. 12, no. 4, pp. 531–540. DOI: 10.17150/2500-4255.2018.12(4).531-540. (In Russian).

Информация об авторе

Жмуров Дмитрий Витальевич – кандидат юридических наук, доцент, доцент кафедры уголовного права, криминологии и уголовного процесса, Институт государстваи права, Байкальский государственный университет, г. Иркутск, ул. Ленина, д. 11; e-mail: zdevraz@ya.ru.

Information about the author

Zhmurov, Dmitriy V. – Ph.D. in Law, Ass. Professor, Chair of Criminal Law, Criminology and Criminal Process, Baikal State University, 11 Lenin st., Irkutsk, 664003, Russian Federation; e-mail: zdevraz@ya.ru.