Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность

УДК 343
doi: 10.35750/2071-8284-2021-1-156-160

Андрей Григорьевич Александров
кандидат юридических наук
ORCID: 0000-0001-5995-7198, ali_a023@mail.ru

Андрей Алексеевич Сафронов
кандидат юридических наук, доцент
ORCID: 0000-0003-4717-6516

Краснодарский университет МВД России
Российская Федерация, 350000, Краснодар, ул. Ярославская, д. 128

Использование сети Даркнет при подготовке и совершении преступлений

Аннотация: В статье авторами рассматривается понятие, сущность, специфика и структурные элементы поверхностной сети (от англ. «surface web») и так называемого глубокого Интернета (от англ. «Deep web»). Рассмотрены особенности использования глубокого Интернета «Deep Web», в котором контент доступен только через подключения, созданные с помощью специального программного обеспечения. В статье рассмотрен тип сети, отделённый от остального общедоступного контента, образующий Даркнет, который уже существовал под названием сеть ARPANET (сеть агентств перспективных исследовательских проектов) до того, как гражданский Интернет, известный нам сегодня, был отделён от неё. Создатели сетей Даркнета не предвидели, сколько применений он найдёт. В статье перечислены программные продукты, используемые для подключения к сети Даркнет. Выявлена цель использования специальных программных продуктов – это обеспечение максимальной анонимности своих пользователей, для значительного затруднения отслеживания их личности, IP-адреса и местоположения в сети. В работе выявлены основные виды преступлений, совершаемых с использованием сети Даркнет, намечены основные направления совершенствования деятельности правоохранительных органов по противодействию преступлениям с использованием ресурсов сети Даркнет. Обозначена проблема развития и увеличения количества преступлений, совершаемых с использованием сети Даркнет.

Ключевые слова: Даркнет, теневой интернет, поверхностная сеть, способ совершения преступления, нелегальные услуги

Для цитирования: Александров А. Г., Сафронов А. А. Использование сети Даркнет при подготовке и совершении преступлений // Вестник Санкт-Петербургского университета МВД России. – 2021. – № 1 (89). – С. 156–160; doi: 10.35750/2071-8284-2021-1-156-160.

Andrey G. Alexandrov
Cand. Sci. (Jurid.), Docent
ORCID: 0000-0001-5995-7198, ali_a023@mail.ru

Andrey A. Safronov
Cand. Sci. (Jurid.), Docent
ORCID: 0000-0003-4717-6516

Krasnodar University of the MIA of Russia
128, str. Yaroslavskaya, Krasnodar, Russian Federation

Use of Darknet to prepare and commit crimes

Abstract: The article examines the concept, essence, specificity, structural elements of the Surface Network (from the English «Surface web») as well as so-called Deep Internet (from the English «Deep web»). The peculiarity of the use of the deep Internet in which the content is available only through connections created with the help of special software is discussed. The article describes the type of network separated from the rest of the public content forming the Darknet. It existed under the name of ARPANET (network of advanced research project agencies) before the civilian Internet known to us today has been separated from it. The creators of the Darknet haven't foreseen all its applications. The paper lists software products used to connect to the Darknet. The purpose of special software products usage is to ensure its users' maximum anonymity to complicate the tracking of their identity, IP-address as well as location in the network. The study reveals the main types of Darknet crimes and outlines ways to improve law enforcement activities to tackle these crimes. In addition, it identifies the problem of development and increasing use of the dark web for criminal purposes.

Keywords: Darknet, shadow Internet, surface network, modus operandi, illegal services

For citation: Alexandrov A. G., Safronov A. A. Use of Darknet to prepare and commit crimes // Vestnik of St. Petersburg University of the Ministry of Internal Affairs of Russia. – 2021. – № 1 (89). – P. 156–160; doi: 10.35750/2071-8284-2021-1-156-160.

Каждый день современный человек пользуется услугами глобальной сети интернет, которую можно назвать открытой. Открывая свои почтовые ящиками, сайты различной тематики или аккаунты, пользователи не осознают тот факт, что всё это лишь небольшая часть глобальной сети, которая называется поверхностной (от англ. «Surface web»). При работе с ней не требуется применения дополнительного программного обеспечения, каких-либо особых программ или средств, в отличие от закрытой сети.

Помимо поверхностной сети «Surface web», существует и теневой, глубокий интернет. Для понимания механизма его использования в целях совершения преступных действий необходимо раскрыть специфику так называемого глубокого интернета (от англ. «Deep web»). Указанная часть глобальной сети Deep Web недоступна для обычного поиска в Интернете. Внутри Deep Web контент работает только через подключения, созданные с помощью специального программного обеспечения. Этот тип сети, отделённый от остального общедоступного контента, образует Даркнет. Его первоначальное название – ARPANET (сеть агентств перспективных исследовательских проектов) до того, как гражданский интернет, известный нам сегодня, был отделён. Популярное ныне название «DarkNet» придумали сотрудники корпорации «Microsoft» в 2002 г. Таких сетей много, и каждая из них доступна благодаря другому программному обеспечению, например I2P (Invisible Internet Project), Freenet или TOR (The Onion Router).

Подсчитано, что среди перечисленных программных продуктов наибольшее количество пользователей имеет программный продукт TOR. Цель TOR – обеспечить анонимность сво-

их пользователей так, чтобы максимально затруднить отслеживание их личности, IP-адреса и местоположения в сети. Суть программы основана на многоуровневом подходе к шифрованию данных.

Программа TOR представляет собой веб-браузер, внешний вид которого основан на популярной бесплатной программе Mozilla Firefox. Особенность веб-адресов в этой сети в том, что они заканчиваются доменным именем первого уровня «onion», что позволяет пользователю скрыть свои данные от интернет-провайдера и получить абсолютную анонимность, используя ресурсы интернета, будучи инкогнито. В данном случае, в отличие от «surface web» пользователю необходимо применять специальные программы, которые и будут обеспечивать режим «инкогнито» и шифровать трафик.

Помимо просмотра специального, закодированного контента, можно также просматривать обычные общедоступные веб-сайты. Доступ к зашифрованному контенту не всегда возможен, и зависит от того, остаётся ли сервер с данным контентом включённым. Это всегда так, потому что узлы связи в значительной степени настроены частными лицами, и их обслуживание связано с большими затратами. Сети типа Даркнета работают намного медленнее, чем обычный Интернет, из-за ограниченной передачи данных. По этой причине страницы обычно выглядят очень скромно, экономично в графических или видеофайлах, часто ограничиваясь только текстом. Более того, коммуникационные узлы запрограммированы пользователями на блокировку по умолчанию методов обмена и распространения файлов, которые вызывают слишком большую передачу данных.

Администраторы сетей внутри Даркнета придерживаются более строгих правил поведения, чем в незашифрованном интернете. В связи со спецификой работы программы TOR среди её пользователей выработался специальный идентификационный признак. В используемом языке существует разделение на «инициированных» пользователей Даркнета и обычных пользователей Интернета. Чрезвычайно сильное чувство анонимности среди пользователей привели к тому, что люди, управляющие страницами, не используют никаких форм цензуры. Это не гарантирует доверия, так как пользователь не является тем, кем он себя называет. По этой причине именно здесь была создана система построения мнений, в которой рекомендации и мнения других пользователей играют важную роль.

Для чего же нужна закрытая сеть внутри глубокого интернета?

Главное – это возможность работать в режиме «инкогнито», однако пользователи начинают заниматься противоправной деятельностью различными способами.

К таковым относится:

1) продажа наркотических средств и психотропных веществ, оружия и боеприпасов;

2) торговля фальшивыми документами, людьми;

3) предоставление услуг наёмных убийц;

4) предоставление за определённую плату пользовательских данных, которые были получены хакерами незаконным способом. В Даркнете можно встретить предложения от очень широкого спектра нелегальных сервисов, не доступных в обычном Интернете, например, по предоставлению услуг по взлому сайтов баз данных. Хакеры рекламируют себя своими навыками, предлагая получить информацию посредством взлома информационных ресурсов частных лиц или компаний.

Использование сети TOR позволяет обмениваться любой информацией на дискуссионных форумах Darknet. Их содержание может быть разнообразным, в т. ч. можно узнать, как построить взрывное устройство из легкодоступных материалов, как получить консультацию для совершения мошенничества посредством социальной инженерии.

Таким образом, можно спровоцировать преступление (склонить другого человека совершить запрещённое действие) или оказать помощь (в данном случае способствовать совершению уголовного преступления путём предоставления рекомендаций или информации). Действия также могут осуществляться в открытой сети Интернет, но выявить ответственных за них людей намного проще.

Важно отметить, что немалую общественную опасность составляют показатели роста преступлений, совершённых как в сфере компьютерной информации, так и преступлений, посягающих на личность, собственность и другие права человека или гражданина с помощью ресурсов сети интернет.

Сложились закономерные формы организации и проведения расследования и раскрытия преступлений, совершённых с помощью сети интернет, но, несмотря на это, важно отметить, что дискуссионным, актуальным и бесспорно сложным вопросом до сих пор остаётся противодействие преступности в закрытой сети – DarkNet.

Для понимания всей сложности ситуации необходимо рассмотреть объёмы преступной деятельности в закрытой сети. Так, А. Л. Осипенко провёл в своей работе контент-анализ Telegram-канала «Black Business», а также пяти Darknet-сайтов (mega darknet market, hydra, matanga, narnia, o3shop, medusa, darkseller, blackmart) [5, с. 138–141]. На момент проведения исследования на данном сайте было размещено примерно 400 предложений:

1) около 200 объявлений было посвящено продаже и распространению наркотических средств и психоактивных веществ;

2) примерно 100 объявлений занимал раздел «Цифровые товары», на котором продавали доступ к сайтам, хранящим взломанные базы данных государственных органов;

3) немалая часть объявлений (около 50) в разделе «Деньги и документы», предлагающих купить документы на право владения транспортным средством.

С. М. Мухин в своём исследовании определил, что DarkNet используют незаконно не только в качестве площадки для предоставления незаконных услуг, но также и для совершения преступления террористического характера [3, с. 110–114]:

1) свободный доступ к схемам и рекомендациям, которые имеют уникальный характер и повышают эффективность террористической деятельности, например, сбыт или легализация полученных преступным путём доходов, шифруемые каналы связи, наём исполнителей и т. д.;

2) более подробные сведения, связанные с изготовлением взрывных устройств и взрывчатых веществ. Информация, позволяющая с легкостью завербовать тех или иных заинтересованных в террористической деятельности лиц и сформировать у них мотивацию на совершение преступлений террористического характера;

3) предоставление возможности спокойно взаимодействовать и контактировать преступным террористическим группам, не опасаясь преследования.

Учитывая данные исследования, необходимо отметить, что наша правоохранительная система не стоит на месте и продолжает борьбу.

Так, более 30 участников межрегиональной преступной группы, занимавшейся клонированием и продажей кредитных и расчётных карт российских и зарубежных банков, были задержаны сотрудниками ФСБ [7]. Среди мошенников были как россияне, так и граждане Украины и Литвы. Нанесённый настоящим владельцам карт ущерб оценивается в сотни миллионов рублей. По данным ФСБ, преступная группа действовала на протяжении как минимум последних трёх лет.

Суть вменяемых её участникам махинаций заключалась в торговле клонированными кредитными и расчётными картами практически всех крупных и средних российских и зарубежных банков.

Необходимые данные реальных владельцев карт преступники получали с помощью доступа к учётным записям пользователей в интернете и платёжным системам.

Проанализировав сложившуюся ситуацию с преступлениями, совершаемыми с помощью сети DarkNet, мы выявили, что, безусловно, правоохранительные органы постоянно работают над их раскрытием и расследованием, но проблема развития и увеличения количества подобных преступлений остаётся.

Для того чтобы решить данную проблему, необходимо обеспечить реализацию таких задач, как:

1) более глубокое и тщательное изучение средств и ресурсов, используемых преступниками в сети DarkNet. Важно отметить, что на данный момент хорошо изучен браузер TOR, но необходимо продолжить расширять знания относительно других браузеров закрытой сети;

2) совершенствование методики и тактики расследования преступлений в данной сфере. Также следует разъяснить законодательно статус информации, полученной из теневого интернета;

3) в целях раскрытия преступлений необходимо ориентировать оперативных сотрудников на общедоступные сети, так как в большинстве случаев преступники используют закрытую сеть только как площадку для совершения преступлений, а наработка клиентской базы происходит в основном в открытой сети.

Создатели сетей Даркнета не предвидели, сколько применений он найдёт. Они даже не могли предположить, насколько этот инструмент упростит задачу злоумышленникам для совершения противоправных действий.

Следует предположить, что в эпоху усиления контроля за общественными процессами и жизнедеятельностью граждан как со стороны государства, так и со стороны крупных корпораций, стремление защитить личную информацию усилится, что приведёт к повсеместному пользованию закрытыми сетями обмена информацией.

Таким образом, с уверенностью можно сказать, что прогресс не стоит на месте, появляются новые составы преступлений, преступники со временем совершают преступления новыми инновационными способами, поэтому главная задача правоохранительных органов – не отставать от быстро развивающейся преступности, не останавливаться на старых методах борьбы с ней. При этом необходимо учитывать опыт практической деятельности сотрудников ОВД, бороться с преступностью передовыми, современными средствами и способами.

Список литературы

1. *Дремлюга Р. И.* Преступный мир Darknet // Юридическая наука и практика. – 2018 – № 1. – С. 52–60.

2. *Мазур А. А.* Актуальные проблемы предупреждения преступности в социальной сети Даркнет // Вестник Российского института кооперации. – 2018. – № 3. – С. 125–129.

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

4. *Осипенко А. Л.* Новые технологии получения и анализа оперативно-розыскной информации: правовые проблемы и перспективы внедрения // Вестник Воронежского института МВД России. – 2015. – № 2. – С. 13–19.

5. *Соловьев В. С., Осипенко А. Л.* Рынок нелегальных товаров и услуг в Darknet и Telegram-каналах / Уголовная политика и культура противодействия преступности : сборник материалов Международной научно-практической конференции. – В 2-х т. – Краснодар: Краснодарский университет МВД России, 2018. – С. 138–141.

6. *Миронов Р. В.* Darknet как источник получения доказательственной и иной информации при расследовании преступлений / Актуальные вопросы юридических наук : материалы V Междунар. науч. конф. (г. Краснодар, июнь 2019 г.). – Краснодар: Новация, 2019. – С. 38–40.

7. *Куликов К. С., Петухов А. Ю.* Основные проблемы выявления и документирования преступлений в сфере незаконного оборота наркотиков, совершаемых в теневом интернете / Актуальные проблемы теории и практики оперативно-розыскной деятельности : сборник материалов VII Всеросс. науч.-практ. конф., посвящ. 100-летию со дня образования службы уголовного розыска. – Краснодар: Краснодарский университет МВД России, 2019. – С. 132–138.

8. *Петухов А. Ю.* Проблемы оперативно-розыскного противодействия лицам, совершающим преступления в сети интернет / Актуальные проблемы теории и практики оперативно-розыскной деятельности : сборник материалов VIII Всеросс. науч.-практ. конф. – Краснодар: Краснодарский университет МВД России, 2020. – С. 169–173.

9. *Рыбенцов А. П., Петухов А. Ю.* Способы идентификации лиц, совершающих преступления в сети интернет / Актуальные проблемы теории и практики оперативно-розыскной деятельности: сборник материалов VIII Всеросс. науч.-практ. конф. – Краснодар: Краснодарский университет МВД России, 2020. – С. 173–176.

10. *Wojciechowski Hubert.* Darknet – wybrane aspekty kryminologiczne, kryminalistyczne i prawne szyfrowanych sieci komputerowych // Acta Universitatis Lodziensis Folia Iuridica 82, 2018.

References

1. *Dremlyuga R. I.* Prestupnyy mir Darknet // Yuridicheskaya nauka i praktika. – 2018 – № 1. – S. 52–60.

2. *Mazur A. A.* Aktual'nyye problemy preduprezhdeniya prestupnosti v sotsial'noy seti Darknet // Vestnik Rossiyskogo instituta kooperatsii. – 2018. – № 3. – S. 125–129.

3. *Mukhin S. M.* Prestupleniya v seti Darknet: kratkaya kharakteristika, problemy protivodeystviya // Al'manakh molodogo issledovatelya. – 2018. – № 5. – S. 110–114.

4. *Osipenko A. L.* Novyye tekhnologii polucheniya i analiza operativno-rozysknoy informatsii: pravovyye problemy i perspektivy vnedreniya // Vestnik Voronezhskogo Instituta MVD Rossii. – 2015. – № 2. – S. 13–19.

5. *Solov'yev V. S.* Rynok nelegal'nykh tovarov i uslug v Darknet i Telegram-kanalakh / V. S. Solov'yev, A. L. Osipenko / Ugolovnaya politika i kul'tura protivodeystviya prestupnosti: sbornik materialov Mezhdunarodnoy nauchno-prakticheskoy konferentsii. – V 2-kh t. – Krasnodar: Krasnodarskiy universitet MVD Rossii, 2018. – S. 138–141.

6. *Mironov R. V.* Darknet kak istochnik polucheniya dokazatel'stvennoy i inoy informatsii pri rassledovanii prestupleniy / Aktual'nyye voprosy yuridicheskikh nauk: materialy V Mezhdunar. nauch. konf. (g. Krasnodar, iyun' 2019 g.). – Krasnodar : Novatsiya, 2019. – S. 38–40.

7. *Kulikov K. S., Petukhov A. Yu.* Osnovnyye problemy vyyavleniya i dokumentirovaniya prestupleniy v sfere nezakonnogo oborota narkotikov, sovershayemykh v tenevom internete / Aktual'nyye problemy teorii i praktiki operativno-rozysknoy deyatel'nosti: sbornik materialov VII Vseross. nauch.-prakt. konf., posvyashch. 100-letiyu so dnya obrazovaniya sluzhby ugolovnogo rozyska. – Krasnodar: Krasnodarskiy universitet MVD Rossii, 2019. – S. 132–138.

8. *Petukhov A. Yu.* Problemy operativno-rozysknogo protivodeystviya litsam, sovershayushchim prestupleniya v seti internet / Aktual'nyye problemy teorii i praktiki operativno-rozysknoy deyatel'nosti: sbornik materialov VIII Vseross. nauch.-prakt. konf. – Krasnodar: Krasnodarskiy universitet MVD Rossii, 2020. – S. 169–173.

9. *Rybentsov A. P., Petukhov A. Yu.* Sposoby identifikatsii lits, sovershayushchikh prestupleniya v seti internet / Aktual'nyye problemy teorii i praktiki operativno-rozysknoy deyatel'nosti: sbornik materialov VIII Vseross. nauch.-prakt. konf. – Krasnodar: Krasnodarskiy universitet MVD Rossii, 2020. – S. 173–176.

10. *Wojciechowski Hubert.* Darknet – wybrane aspekty kryminologiczne, kryminalistyczne i prawne szyfrowanych sieci komputerowych // Acta Universitatis Lodziensis Folia Iuridica 82, 2018.

Статья поступила в редакцию 28.10.2020; одобрена после рецензирования 19.01.2021; принята к публикации 02.03.2021.